

全国计算机技术与软件专业技术资格（水平）考试指定用书

# 网络工程师 2009至2016年试题分析与解答

全国计算机专业技术资格考试办公室 主编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

# 网络工程师
# 2009至2016年试题分析与解答

全国计算机专业技术资格考试办公室 主编

清华大学出版社
北京

## 内 容 简 介

网络工程师考试是全国计算机技术与软件专业技术资格（水平）考试的中级职称考试，是历年各级考试报名中最大的热点之一。本书汇集了 2009 上半年到 2016 下半年的所有试题和权威的解析，参加考试的考生，认真读懂本书的内容后，将会更加了解考题的思路，对提升自己考试通过率的信心会有极大的帮助。



**图书在版编目（CIP）数据**

网络工程师 2009 至 2016 年试题分析与解答 / 全国计算机专业技术资格考试办公室主编. —北京：清华大学出版社，2017
（全国计算机技术与软件专业技术资格（水平）考试指定用书）
ISBN 978-7-302-48587-2

Ⅰ. ①网…　Ⅱ. ①全…　Ⅲ. ①计算机网络 – 资格考试 – 题解　Ⅳ. ①TP393-44

中国版本图书馆 CIP 数据核字（2017）第 250000 号

**责任编辑：**杨如林　柴文强
**封面设计：**常雪影
**责任校对：**徐俊伟
**责任印制：**刘海龙

**出版发行：**清华大学出版社
**网　　址：**http://www.tup.com.cn, http://www.wqbook.com
**地　　址：**北京清华大学学研大厦 A 座　　**邮　　编：**100084
**社 总 机：**010-62770175　　**邮　　购：**010-62786544
**投稿与读者服务：**010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈：**010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 装 者：**清华大学印刷厂
**经　　销：**全国新华书店
**开　　本：**185mm×230mm　**印　　张：**49.25　**防伪页：**1　**字　　数：**1048 千字
**版　　次：**2017 年 11 月第 1 版　　**印　　次：**2017 年 11 月第 1 次印刷
**印　　数：**1～3000
**定　　价：**99.00 元

---

产品编号：075341-01

# 前　言

根据国家有关的政策性文件，全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）已经成为计算机软件、计算机网络、计算机应用、信息系统、信息服务领域高级工程师、工程师、助理工程师、技术员国家职称资格考试。而且，根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师、系统架构设计师和信息系统项目管理师等资格的考试标准已经实现了中国与日本互认，程序员和软件设计师等资格的考试标准已经实现了中国和韩国互认。

计算机软件考试规模发展很快，年报考规模已经超过 30 万人，二十多年来，累计报考人数超过 470 万人。

计算机软件考试已经成为我国著名的 IT 考试品牌，其证书的含金量之高已得到社会的公认。计算机软件考试的有关信息见网站www.ruankao.org.cn中的资格考试栏目。

对考生来说，学习历年试题分析与解答是理解考试大纲的最有效、最具体的途径。

为帮助考生复习备考，全国计算机专业技术资格考试办公室组织汇集了网络工程师 2009 至 2016 年的试题分析与解答，以便于考生测试自己的水平，发现自己的弱点，更有针对性、更系统地学习。

计算机软件考试的试题质量高，包括了职业岗位所需的各个方面的知识和技术，不但包括技术知识，还包括法律法规、标准、专业英语、管理等方面的知识；不但注重广度，而且还有一定的深度；不但要求考生具有扎实的基础知识，还要具有丰富的实践经验。

这些试题中，包含了一些富有创意的试题，一些与实践结合得很好的试题，一些富有启发性的试题，具有较高的社会引用率，对学校教师、培训指导者、研究工作者都是很有帮助的。

由于作者水平有限，时间仓促，书中难免有错误和疏漏之处，诚恳地期望各位专家和读者批评指正，对此，我们将深表感激。

编者

2017 年 8 月

# 目　　录

# 第 1 章　2009 上半年网络工程师上午试题分析与解答

**试题（1）**

___（1）___是指按内容访问的存储器。

（1）A. 虚拟存储器　　　　B. 相联存储器
　　C. 高速缓存（Cache）　D. 随机访问存储器

**试题（1）分析**

本题考查计算机系统存储器方面的基础知识。

计算机系统的存储器按所处的位置可分为内存和外存。按构成存储器的材料，可分为磁存储器、半导体存储器和光存储器。按存储器的工作方式可分为读写存储器和只读存储器。按访问方式可分为按地址访问的存储器和按内容访问的存储器。按寻址方式可分为随机存储器、顺序存储器和直接存储器。

相联存储器是一种按内容访问的存储器。

**参考答案**

（1）B

**试题（2）**

处理机主要由处理器、存储器和总线组成。总线包括___（2）___。

（2）A. 数据总线、地址总线、控制总线　B. 并行总线、串行总线、逻辑总线
　　C. 单工总线、双工总线、外部总线　D. 逻辑总线、物理总线、内部总线

**试题（2）分析**

本题考查计算机系统总线和接口方面的基础知识。

广义地讲，任何连接两个以上电子元器件的导线都可以称为总线。通常可分为 4 类：

① 芯片内总线。用于在集成电路芯片内部各部分的连接。

② 元件级总线。用于一块电路板内各元器件的连接。

③ 内总线，又称系统总线。用于构成计算机各组成部分（CPU、内存和接口等）的连接。

④ 外总线，又称通信总线。用计算机与外设或计算机与计算机的连接或通信。

连接处理机的处理器、存储器及其他部件的总线属于内总线，按总线上所传送的内容分为数据总线、地址总线和控制总线。

**参考答案**

（2）A

**试题（3）**

计算机中常采用原码、反码、补码和移码表示数据，其中，±0 编码相同的是__（3）__。

（3）A. 原码和补码　　B. 反码和补码

C. 补码和移码　　D. 原码和移码

**试题（3）分析**

本题考查计算机系统数据编码基础知识。

设机器字长为 $n$（即采用 $n$ 个二进制位表示数据），最高位是符号位，0 表示正号，1 表示负号。

原码表示方式下，除符号位外，$n$–1 位表示数值的绝对值。因此，$n$ 为 8 时，$[+0]_{原}$=0 0000000，$[-0]_{原}$=1 0000000 $[+0]_{原}$=0 0000000，$[-0]_{原}$=1 0000000 。

正数的反码与原码相同，负数的反码则是其绝对值按位求反。$n$ 为 8 时，数值 0 的反码表示有两种形式：$[+0]_{反}$=0 0000000，$[-0]_{反}$=1 1111111 。

正数的补码与其原码和反码相同，负数的补码则等于其反码的末尾加 1。在补码表示中，0 有唯一的编码：$[+0]_{原}$=0 0000000，$[-0]_{原}$=00000000 。

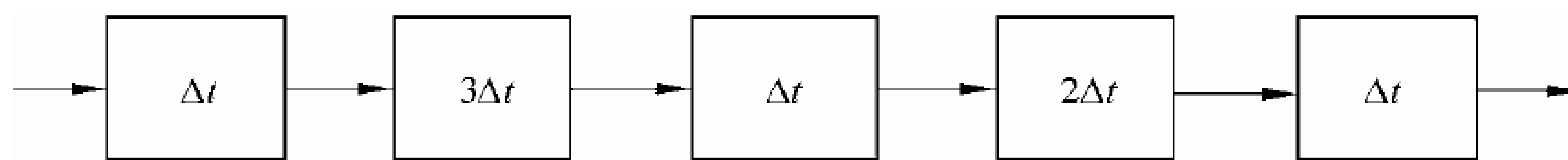
移码表示法是在数 X 上增加一个偏移量来定义的，常用于表示浮点数中的阶码。机器字长为 $n$ 时，在偏移量为 $2^{n-1}$ 的情况下，只要将补码的符号位取反便可获得相应的移码表示。

**参考答案**

（3）C

**试题（4）**

某指令流水线由 5 段组成，第 1、3、5 段所需时间为 $\Delta t$，第 2、4 段所需时间分别为 $3\Delta t$、$2\Delta t$，如下图所示，那么连续输入 $n$ 条指令时的吞吐率（单位时间内执行的指令个数）$TP$ 为__（4）__。




（4）A. $\dfrac{n}{5*(3+2)\Delta t}$　　B. $\dfrac{n}{(3+3+2)\Delta t+3(n-1)\Delta t}$

C. $\dfrac{n}{(3+2)\Delta t+(n-3)\Delta t}$　　D. $\dfrac{n}{(3+2)\Delta t+5*3\Delta t}$

**试题（4）分析**

本题考查计算机系统流水线方面的基础知识。

吞吐率和建立时间是使用流水线技术的两个重要指标。吞吐率是指单位时间里流水线处理机流出的结果数。对指令而言，就是单位时间里执行的指令数。流水线开始工作，须经过一定时间才能达到最大吞吐率，这就是建立时间。若 $m$ 个子过程所用时间一样，

均为 $\Delta t_0$，则建立时间 $T_0 = m\Delta t_0$。

本题目中，连续输入 $n$ 条指令时，第 1 条指令需要的时间为 $(1+3+1+2+1)\Delta t$，之后，每隔 $3\Delta t$ 便完成 1 条指令，即流水线一旦建立好，其吞吐率为最长子过程所需时间的倒数。综合 $n$ 条指令的时间为 $(1+3+1+2+1)\Delta t + (n-1)\times 3\Delta t$，因此吞吐率为

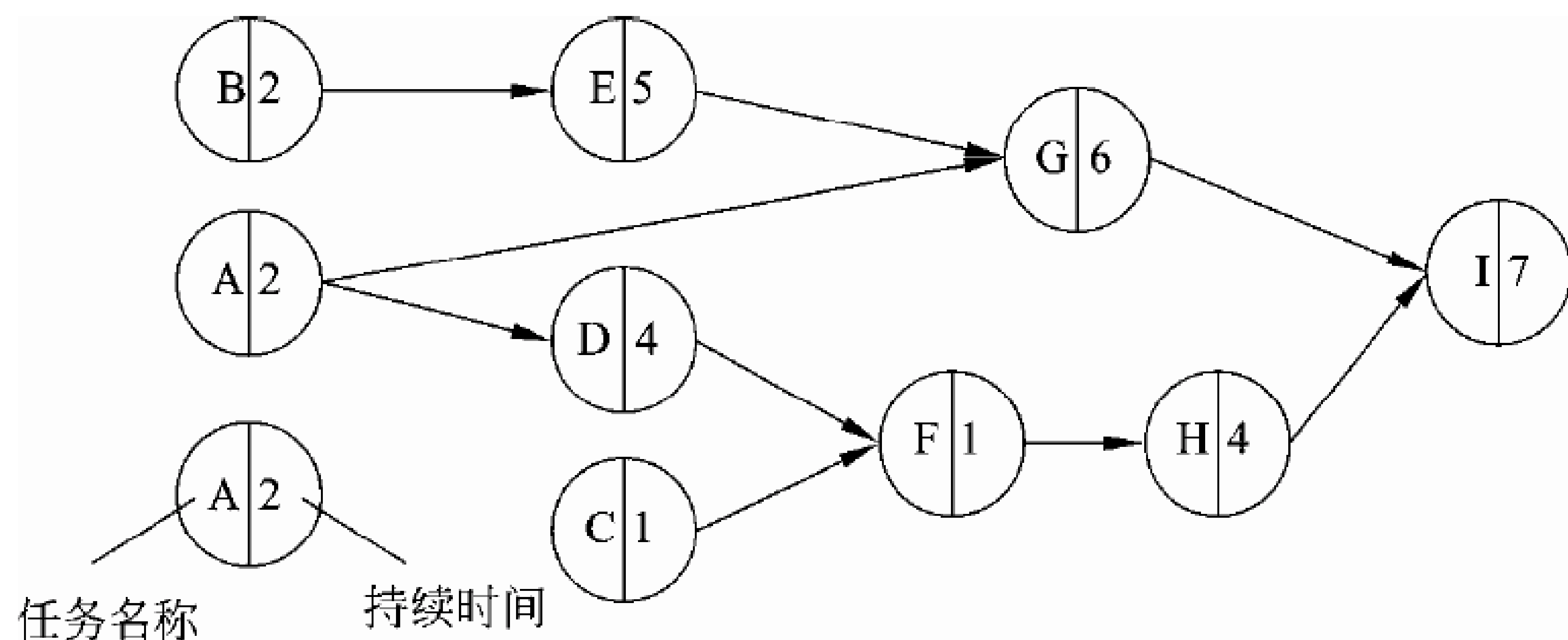
$$\frac{n}{(3+3+2)\Delta t + 3(n-1)\Delta t}$$

**参考答案**

（4）B

**试题（5）、（6）**

某项目主要由 A～I 任务构成，其计划图（如下图所示）展示了各任务之间的前后关系以及每个任务的工期（单位：天），该项目的关键路径是__（5）__。在不延误项目总工期的情况下，任务 A 最多可以推迟开始的时间是__（6）__天。




（5）A.  A→G→I　　　　B.  A→D→F→H→I

　　C.  B→E→G→I　　　　D.  C→F→H→I

（6）A. 0　　B. 2　　C. 5　　D. 7

**试题（5）、（6）分析**

本题考查项目计划的关键路径和松弛时间。图中任务流 A→G→I 的持续时间为 15；任务流 A→D→F→H→I 的持续时间为 18；任务流 B→E→G→I 的持续时间为 20；任务流 C→F→H→I 的持续时间为 13。因此关键路径为 B→E→G→I，其持续时间是 20。任务 A 处于任务流 A→G→I 和任务流 A→D→F→H→I 中，分别持续时间为 15 和 18，因此任务 A 的可延迟开始时间为 2。

**参考答案**

（5）C　　（6）B

**试题（7）**

软件风险一般包含__（7）__两个特性。

（7）A.  救火和危机管理　　　　B.  已知风险和未知风险

C. 不确定性和损失　　　　　D. 员工和预算

**试题（7）分析**

本题考查软件风险的特性。

软件风险一般包括不确定性和损失两个特性，其中不确定性是指风险可能发生，也可能不发生；损失是当风险确实发生时，会引起的不希望的后果和损失。救火和危机管理是对不适合但经常采用的软件风险管理策略。已知风险和未知风险是对软件风险进行分类的一种方式。员工和预算是在识别项目风险时需要识别的因素。

**参考答案**

（7）C

**试题（8）、（9）**

设系统中有 R 类资源 m 个，现有 n 个进程互斥使用。若每个进程对 R 资源的最大需求为 w，那么当 m、n、w 取下表的值时，对于下表中的 a～e 五种情况，__（8）__两种情况可能会发生死锁。对于这两种情况，若将__（9）__，则不会发生死锁。

| | a | b | c | d | e |
|---|---|---|---|---|---|
| m | 2 | 2 | 2 | 4 | 4 |
| n | 1 | 2 | 2 | 3 | 3 |
| w | 2 | 1 | 2 | 2 | 3 |

（8）A. a 和 b　　B. b 和 c　　C. c 和 d　　D. c 和 e

（9）A. n 加 1 或 w 加 1　　B. m 加 1 或 w 减 1

C. m 减 1 或 w 加 1　　D. m 减 1 或 w 减 1

**试题（8）、（9）分析**

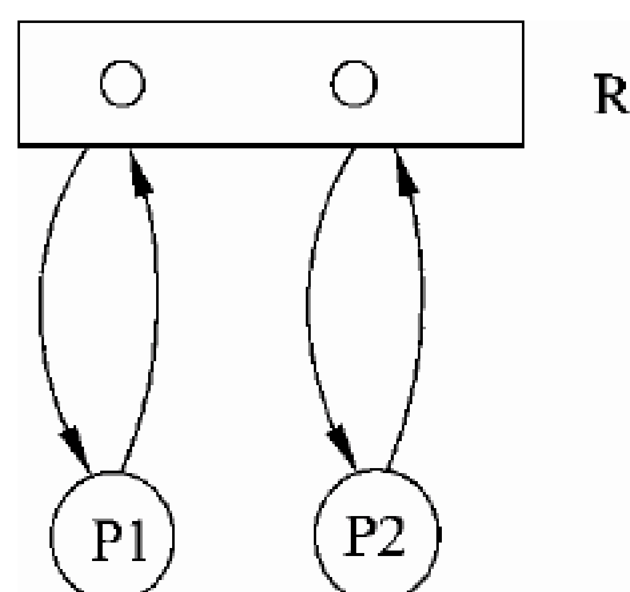
本题考查对操作系统死锁方面基本知识掌握的程度。系统中同类资源分配不当会引起死锁。一般情况下，若系统中有 m 个单位的存储器资源，它被 n 个进程使用，当每个进程都要求 w 个单位的存储器资源，当 m<nw 时，可能会引起死锁。

试题（8）分析如下：

情况 a：m=2，n=1，w=2，系统中有两个资源，1 个进程使用，该进程最多要求两个资源，所以不会发生死锁。

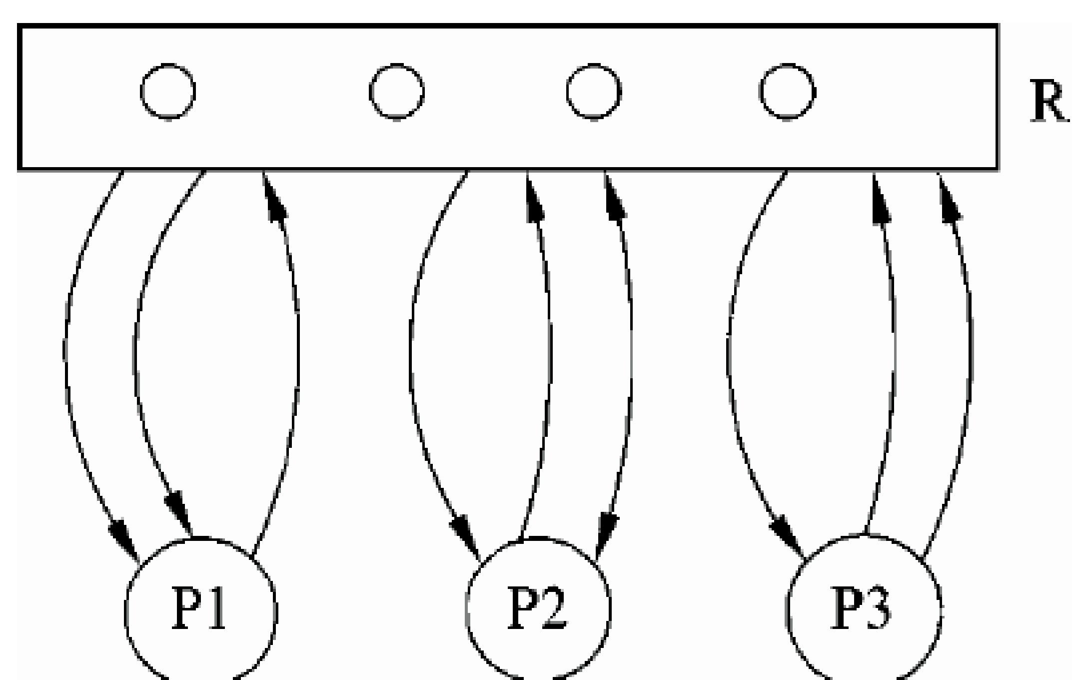
情况 b：m=2，n=2，w=1，系统中有两个资源，两个进程使用，每个进程最多要求 1 个资源，所以不会发生死锁。

情况 c：m=2，n=2，w=2，系统中有两个资源，两个进程使用，每个进程最多要求两个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配 1 个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁，这时进程资源图如下图所示。




情况 d：m=4，n=3，w=2，系统中有 4 个资源，3 个进程使用，每个进程最多要求两个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配 1 个资源，此时，系统中还剩 1 个资源，可以使其中的一个进程得到所需资源并运行完毕，所以不会发生死锁。

情况 e：m=4，n=3，w=3，系统中有 4 个资源，3 个进程使用，每个进程最多要求 3 个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配 1 个，第二轮系统先为一个进程分配 1 个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁，这时进程资源图如下图所示。




试题（9）分析如下：

对于 c 和 e 两种情况，若将 m 加 1，则情况 c：　m=3，n=2，w=2，系统中有 3 个资源，两个进程使用，每个进程最多要求两个资源，系统先为每个进程分配 1 个，此时，系统中还剩 1 个可供分配的资源，使得其中的一个进程能得到所需资源执行完，并释放所有资源使另一个进程运行完毕；若将 w 减 1，则情况 c：　m=2，n=2，w=1，系统中有两个资源，两个进程各需一个，系统为每个进程分配 1 个，此时，进程都能运行完，显然不会发生死锁。情况 e 分析同理。

**参考答案**

（8）D　（9）B

**试题（10）**

关于软件著作权产生的时间，表述正确的是＿（10）＿。

（10）A. 自作品首次公开发表时

B. 自作者有创作意图时

C. 自作品得到国家著作权行政管理部门认可时

D. 自作品完成创作之日

**试题（10）分析**

本题考查知识产权中关于软件著作权方面的知识。

在我国，软件著作权采用“自动保护”原则。《计算机软件保护条例》第十四条规定：“软件著作权自软件开发完成之日起产生。”即软件著作权自软件开发完成之日起自动产生，不论整体还是局部，只要具备了软件的属性即产生软件著作权，既不要求履行任何形式的登记或注册手续，也无须在复制件上加注著作权标记，也不论其是否已经发表都依法享有软件著作权。

一般来讲，一个软件只有开发完成并固定下来才能享有软件著作权。如果一个软件一直处于开发状态中，其最终的形态并没有固定下来，则法律无法对其进行保护。因此，条例（法律）明确规定软件著作权自软件开发完成之日起产生。当然，现在的软件开发经常是一项系统工程，一个软件可能会有很多模块，而每一个模块能够独立完成某一项功能。自该模块开发完成后就产生了著作权。所以说，自该软件开发完成后就产生了著作权。

**参考答案**

（10）D

**试题（11）、（12）**

E载波是ITU-T建议的传输标准，其中E3信道的数据速率大约是__（11）__Mb/s。贝尔系统T3信道的数据速率大约是__（12）__Mb/s。

（11）A. 64　　B. 34　　C. 8　　D. 2

（12）A. 1.5　　B. 6.3　　C. 44　　D. 274

**试题（11）、（12）分析**

E载波是ITU-T建议的数字传输标准，分为5个复用级别。在E1信道中，8位组成一个时槽，32个时槽（TS0～TS31）组成一个帧，16个帧组成一个复帧。在E1帧中，TS0用于帧控制，TS16用于随路信令和复帧控制，其余的30个时槽用于传送话音和数据。

E1载波的数据速率为2.048Mb/s，其中每个信道的数据速率是64kb/s。

E2信道由4个E1信道组成，数据速率为8.448Mb/s。

E3信道由16个E1信道组成，数据速率为34.368Mb/s。

E4信道由4个E3信道组成，数据速率为139.264Mb/s。

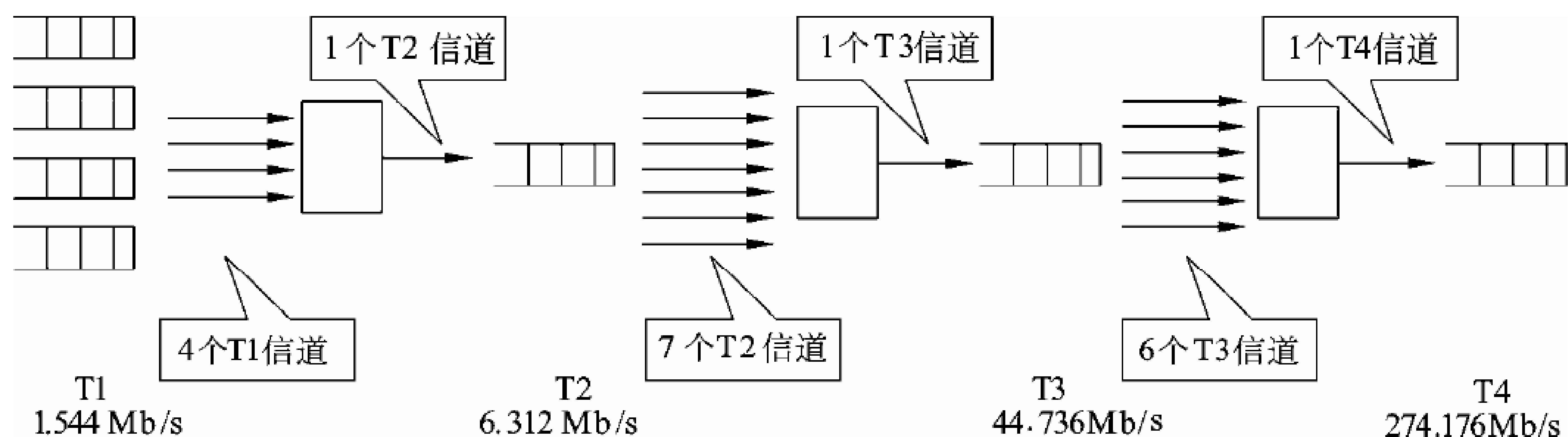
E5信道由4个E4信道组成，数据速率为565.148Mb/s。

T载波是贝尔系统的数字传输标准（如下图所示），在北美和日本使用。T载波中话音信道的数据速率为56kb/s。24路话音被复合在一条T1信道上，其数据速率为1.544Mb/s。

T2信道由4个T1信道组成，数据速率为6.312Mb/s。

T3信道由7个T2信道组成，数据速率为44.736Mb/s。

T4 信道由 6 个 T3 信道组成，数据速率为 274.176Mb/s。




T 载波系统示意图

**参考答案**

（11）B　（12）C

**试题（13）、（14）**

RS-232-C 的电气特性采用 V.28 标准电路，允许的数据速率是＿（13）＿，传输距离不大于＿（14）＿。

（13）A. 1kb/s　B. 20kb/s　C. 100kb/s　D. 1Mb/s

（14）A. 1m　B. 15m　C. 100m　D. 1km

**试题（13）、（14）分析**

物理层标准规定了 DTE 与 DCE 之间接口的机械特性、电气特性、功能特性和过程特性。RS-232-C 是主要的物理层接口之一，是 PC 的标准设备。RS-232-C 的机械特性没有规定，可以采用 25 针、15 针或 9 针 D 型连接器，RS-232-C 的电气特性与 CCITT V.28 标准兼容。常用的各种电气特性标准参见下表。

**三种电气特性标准比较**

| 标　准 | 信号“1” | 信号“0” | 数据速率 | 距　离 | 电路技术 |
|---|---|---|---|---|---|
| CCITT V.10/X.26 | –4V～–6V | +4V～+6V | ≤300kb/s | 1 000m (<3kb/s)<br>10m (300kb/s) | IC |
| CCITT V.11/X.27 | –2V～–6V | +2V～+6V | 10Mb/s | 1 000m (≤100kb/s)<br>10 m (10Mb/s) | IC |
| CCITT V.28 | –3V～–15V | +3V～+15V | 20kb/s | 15 m | 分立元件 |

**参考答案**

（13）B　（14）B

**试题（15）、（16）**

曼彻斯特编码的特点是＿（15）＿，它的编码效率是＿（16）＿。

（15）A. 在“0”比特的前沿有电平翻转，在“1”比特的前沿没有电平翻转

B. 在“1”比特的前沿有电平翻转，在“0”比特的前沿没有电平翻转

C. 在每个比特的前沿有电平翻转

D. 在每个比特的中间有电平翻转

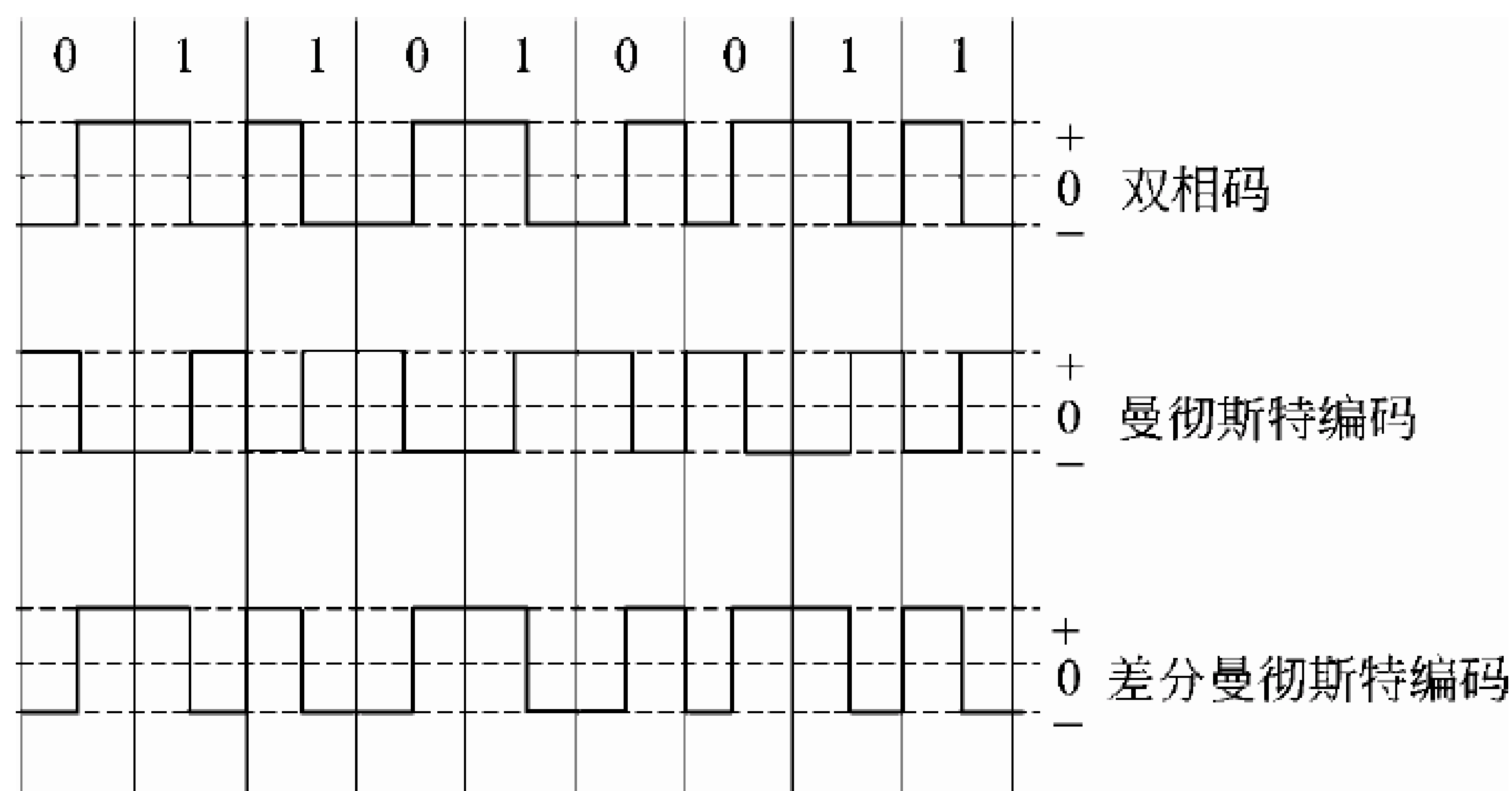
（16）A. 50%　　B. 60%　　C. 80%　　D. 100%

**试题（15）、（16）分析**

曼彻斯特编码（Manchester Code）是一种双相码（或称分相码）。双相码要求每一位中间都要有一个电平转换，因而这种代码的优点是自定时，同时双相码也有检测差错的功能，如果某一位中间缺少了电平翻转，则被认为是违例代码。在下图中，我们用高电平到低电平的转换边表示“0”，而低电平到高电平的转换边表示“1”，相反的表示也是允许的。比特中间的电平转换既表示了数据代码，同时也作为定时信号使用。曼彻斯特编码用在以太网中。

差分曼彻斯特编码类似于曼彻斯特编码，它把每一比特的起始边有无电平转换作为区分“0”和“1”的标志，这种编码用在令牌环网中。

在曼彻斯特编码和差分曼彻斯特编码中，每比特中间都有一次电平跳变，因此波特率是数据速率的两倍。对于 100Mb/s 的高速网络，如果采用这类编码方法，就需要 200M 的波特率，其硬件成本是 100M 波特率硬件成本的 5～10 倍。作为一种变通的办法，可以使用 4B/5B 或 8B/10B 编码。




曼彻斯特编码示意图

**参考答案**

（15）D　　（16）A

**试题（17）、（18）**

HDLC 协议是一种__（17）__，采用__（18）__标志作为帧定界符。

（17）A. 面向比特的同步链路控制协议

B. 面向字节计数的同步链路控制协议

C. 面向字符的同步链路控制协议

D. 异步链路控制协议

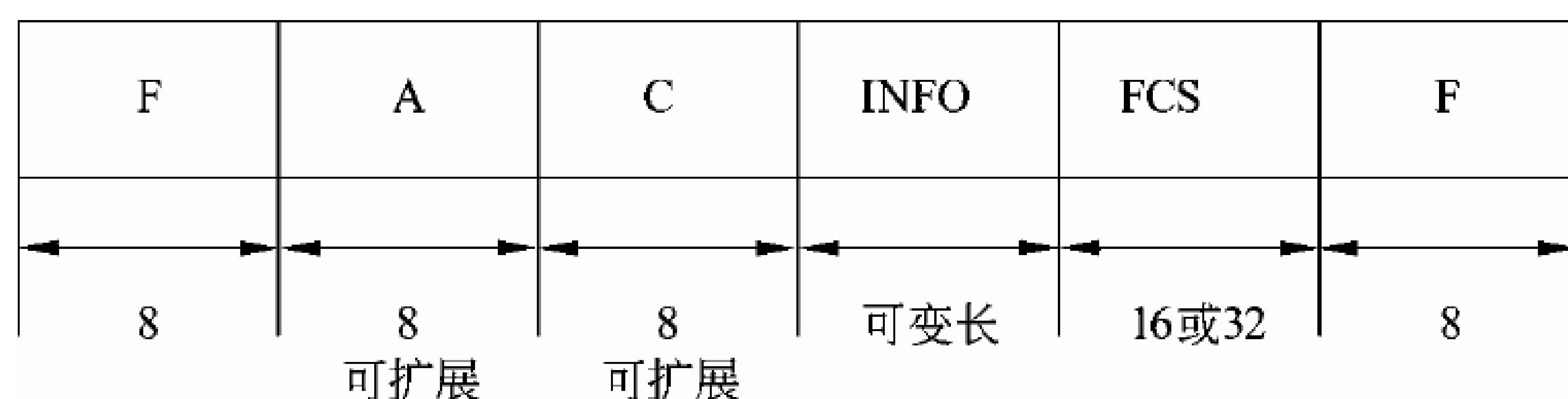
（18）A. 10000001　　B. 01111110　　C. 10101010　　D. 10101011

**试题（17）、（18）分析**

数据链路控制协议分为面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，并用 10 个专用字符控制传输过程。面向比特的协议以比特作为传输的基本单位，它的传输效率高，广泛地应用于公用数据网中。

HDLC（High Level Data Link Control，高级数据链路控制）协议是 ISO 根据 IBM 公司的 SDLC（Synchronous Data Link Control）协议扩充开发而成的。美国国家标准化协会（ANSI）则根据 SDLC 开发出类似的协议，叫作 ADCCP 协议（Advanced Data Communication Control Procedure）。

HDLC 使用统一的帧结构进行同步传输，下图为 HDLC 帧的格式示意图。HDLC 帧由 6 个字段组成，以两端的标志字段（F）作为帧的边界，在信息字段（INFO）前面的三个字段（F、A 和 C）叫作帧头，信息字段后面的两个字段（FCS 和 F）叫作帧尾，信息字段中包含了要传输的数据。




HDLC 帧结构示意图

HDLC 用一种特殊的比特模式 01111110 作为标志以确定帧的边界。同一个标志既可以作为前一帧的结束，也可以作为后一帧的开始。链路上所有的站都在不断地探索标志模式，一旦得到一个标志就开始接收帧。在接收帧的过程中如果发现一个标志，则认为该帧结束了。如果帧中间出现比特模式 01111110 时，也会被当作标志，从而破坏了帧的同步。为了避免这种错误，要使用位填充技术，即发送站的数据比特序列中一旦发现 0 后有 5 个 1，则在第 7 位插入一个 0。这样就保证了传输的数据比特序列中不会出现与帧标志相同的比特模式。接收站则进行相反的操作：在接收的比特序列中如果发现 0 后有 5 个 1，则检查第 7 位，若第 7 位为 0 则删除之；若第 7 位是 1 且第 8 位是 0，则认为是检测到帧尾的标志域；若第 7 位和第 8 位都是 1，则认为是发送站的停止信号。

**参考答案**

（17）A　（18）B

**试题（19）**

设信道带宽为 3400Hz，采用 PCM 编码，采样周期为 125μs，每个样本量化为 128 个等级，则信道的数据速率为<u>（19）</u>。

（19）A. 10Kb/s　　B. 16Kb/s　　C. 56Kb/s　　D. 64Kb/s

**试题（19）分析**

模拟信号通过数字信道传输具有效率高、失真小的优点，而且可以开发新的通信业务。常用的数字化技术就是脉冲编码调制技术（Pulse Code Modulation，PCM），简称脉码调制。PCM主要经过3个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组输出。

采样的频率决定了恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

$$f=\frac{1}{T}\geqslant 2f_{max}$$

其中，$f$为采样频率，$T$为采样周期，$f_{max}$为信号的最高频率。

电话线路中带通滤波器的带宽为3kHz（即300～3300Hz）。根据Nyquist采样定理，最小采样频率应为6600 Hz，CCITT规定话音信号的采样频率为8kHz。采样后得到的样本必须通过四舍五入量化为离散值，离散值的个数决定了量化的精度。在T1系统中采用128级量化，每个样本用7位二进制数字表示，在数字信道上传输这种数字化了的话音信号的速率是7×8000=56kb/s。在E1系统中采用256级量化，每个样本用8位二进制数字表示，传输速率为64kb/s。

**参考答案**

（19）C

**试题（20）**

设数据码字为10010011，采用海明码进行校验，则必须加入__（20）__比特冗余位才能纠正一位错。

（20）A. 2　　B. 3　　C. 4　　D. 5

**试题（20）分析**

海明（Hamming）研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字，码字之间的海明距离是一个码字变成另一个码字时必须改变的最小位数。海明用数学分析的方法说明了海明距离的几何意义，$n$位的码字可以用$n$维空间的超立方体的一个顶点来表示，两个码字之间的海明距离就是超立方体的两个对应顶点之间的一条边，而且这是两顶点（从而两个码字）之间的最短距离，出错的位数小于这个距离都可以被判断为就近的码字。这就是海明码纠错的原理，它用码位的增加（因而通信量的增加）来换取正确率的提高。

按照海明的理论，纠错编码就是把所有合法的码字尽量安排在$n$维超立方体的顶点上，使得任一对码字之间的距离尽可能大。如果任意两个码字之间的海明距离是$d$，则

所有少于等于 $d-1$ 位的错误都可以检查出来，所有少于 $d/2$ 位的错误都可以纠正。

如果对于 $m$ 位的数据，增加 $k$ 位冗余位，则组成 $n=m+k$ 位的纠错码。对于 $2^m$ 个有效码字中的每一个，都有 $n$ 个无效但可以纠错的码字，这些可纠错的码字与有效码字的距离是 1，含单个出错位。这样，对于一个有效的消息总共有 $n+1$ 个可识别的码字。这 $n+1$ 个码字相对于其他 $2^m-1$ 个有效消息的距离都大于 1。这意味着总共有 $2^m(n+1)$个有效的或是可纠错的码字。显然这个数应小于等于码字的所有可能的个数，即 $2^n$。于是，有

$$2^m(n+1)<2^n$$

因为 $n=m+k$，得出

$$m+k+1<2^k$$

对于给定的数据位 $m$，上式给出了 $k$ 的下界，即要纠正单个错误，$k$ 必须取的最小值。

在本题中，数据码字为 10010011 的 $m=8$，由上式计算出的 $k$ 的最小值应为 4。

**参考答案**

（20）C

**试题（21）**

可以把所有使用 DHCP 协议获取 IP 地址的主机划分为不同的类别进行管理。下面的选项列出了划分类别的原则，其中合理的是__（21）__。

（21）A. 移动用户划分到租约期较长的类

B. 固定用户划分到租约期较短的类

C. 远程访问用户划分到默认路由类

D. 服务器划分到租约期最短的类

**试题（21）分析**

动态主机配置协议（DHCP）用于在大型网络中为客户端自动分配 IP 地址及有关网络参数（默认网关和 DNS 服务器地址等）。使用 DHCP 服务器便于进行网络管理，可以节省网络配置的工作量，有效地避免网络地址冲突，还能解决 IP 地址资源不足的问题。

DHCP 租约周期是 IP 地址的有效期。租约周期可长可短，取决于用户的上网环境和工作性质。一般把移动用户划分到租约期较短的管理类，把固定用户划分到租约期较长的管理类，远程访问用户划分到默认路由类。对于服务器主机则要为其保留固定的 IP 地址，并且要把保留的 IP 地址与服务器主机的 MAC 地址进行绑定。

**参考答案**

（21）C

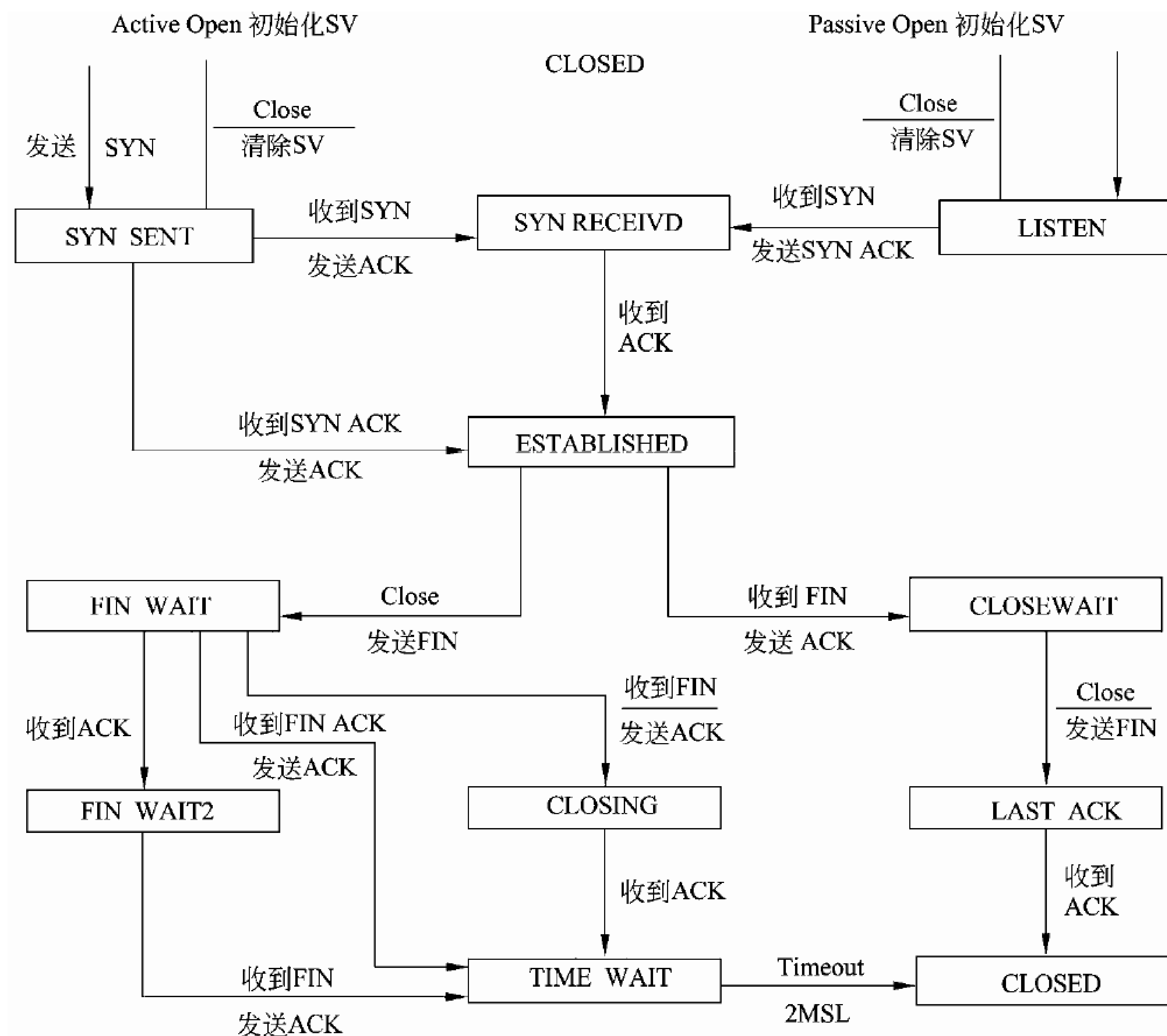
**试题（22）**

TCP 协议在建立连接的过程中可能处于不同的状态，用 netstat 命令显示出 TCP 连接的状态为 SYN_SEND，则这个连接正处于__（22）__。

（22）A. 监听对方的建立连接请求　　　B. 已主动发出连接建立请求

C. 等待对方的连接释放请求　　　　D. 收到对方的连接建立请求

**试题（22）分析**




TCP 的连接状态图示意图

上图表示 TCP 的连接状态图。事实上，在 TCP 协议运行过程中，有多个连接处于不同的状态。当 TCP 处于 SYN_SEND 状态时，表示协议实体已主动发出连接建立请求。

**参考答案**

（22）B

**试题（23）、（24）**

Tracert 命令通过多次向目标发送＿（23）＿来确定到达目标的路径，在连续发送的多个 IP 数据包中，＿（24）＿字段都是不同的。

（23）A. ICMP 地址请求报文　　B. ARP 请求报文
　　　C. ICMP 回声请求报文　　D. ARP 响应报文

（24）A. 源地址　　B. 目标地址　　C. TTL　　D. ToS

**试题（23）、（24）分析**

Tracert 命令的功能是确定到达目标的路径，并显示通路上每一个中间路由器的 IP 地址。通过多次向目标发送 ICMP 回声（echo）请求报文，每次增加 IP 头中 TTL 字段的值，就可以确定到达各个路由器的时间。显示的地址是路由器接近源的这一边的端口地址。Tracert 命令的语法如下：

```
tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]
```

对以上参数解释如下：

- -d

不进行名字解析，显示中间节点的 IP 地址，这样可以加快跟踪的速度。

- -h MaximumHops

说明地址搜索的最大跃点数，默认值是 30 跳。

- -j HostList

说明发送回声请求报文要使用 IP 头中的松散源路由选项，标识符 HostList 列出必须经过的中间节点的地址或名字，最多可以列出 9 个中间节点，各个中间节点用空格隔开。

- -w Timeout

说明等待 ICMP 回声响应报文的时间（μs），如果接收超时，则显示星号“*”，默认超时间隔是 4s。

- TargetName

用 IP 地址或主机名表示的目标。

这个诊断工具通过多次发送 ICMP 回声请求报文来确定到达目标的路径，每个报文中的 TTL 字段的值都是不同的。通路上的路由器在转发 IP 数据报之前先要对 TTL 字段减一，如果 TTL 为 0，则路由器就向源端返回一个超时（Time Exceeded）报文，并丢弃原来要转发的报文。在 tracert 第一次发送的回声请求报文中置 TTL=1，然后每次加 1，这样就能收到沿途各个路由器返回的超时报文，直至收到目标返回的 ICMP 回声响应报文。如果有的路由器不返回超时报文，那么这个路由器就是不可见的，显示列表中用星号“*”表示之。

举例如下：

（1）要跟踪到达主机 corp7.microsoft.com 的路径，则键入：

tracert corp7.microsoft.com

（2）要跟踪到达主机 corp7.microsoft.com 的路径，并且不进行名字解析，只显示中间节点的 IP 地址，则键入：

tracert -d corp7.microsoft.com

（3）要跟踪到达主机 corp7.microsoft.com 的路径，并使用松散源路由，则键入：

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 corp7.microsoft.com

下图是利用命令 tracert www.163.com.cn 显示的路由跟踪列表。

```
C:\Documents and Settings\Administrator>tracert www.163.com.cn

Tracing route to www.163.com.cn [219.137.167.157]
over a maximum of 30 hops:

  1    26 ms    15 ms    11 ms  100.100.17.254
  2    <1 ms    <1 ms    <1 ms  254-20-168-128.cos.it-comm.net [128.168.20.254]

  3    <1 ms    <1 ms    <1 ms  61.150.43.65
  4    <1 ms    <1 ms    <1 ms  222.91.155.5
  5    <1 ms    <1 ms    <1 ms  125.76.189.81
  6     1 ms    <1 ms    <1 ms  61.134.0.13
  7    28 ms    28 ms    28 ms  202.97.35.229
  8    28 ms    29 ms    29 ms  61.144.3.17
  9    29 ms    29 ms    32 ms  61.144.5.9
 10    32 ms    32 ms    32 ms  219.137.11.53
 11    29 ms    29 ms    28 ms  219.137.167.157

Trace complete.
```

tracert 的显示结果

**参考答案**

（23）C　（24）C

**试题（25）、（26）**

OSPF 协议适用于 4 种网络。下面的选项中，属于广播多址网络（Broadcast Multi-Access）的是__（25）__，属于非广播多址网络（None Broadcast Multi-Access）的是__（26）__。

（25）A. Ethernet　B. PPP　C. Frame Relay　D. RARP

（26）A. Ethernet　B. PPP　C. Frame Relay　D. RARP

**试题（25）、（26）分析**

OSPF 定义了 4 种网络：

（1）广播多址网络（Broadcast Multi-Access），例如 Ethernet、Token Ring 和 FDDI 等。

（2）非广播多址网络（None Broadcast Multi-Access，NBMA），例如 Frame Relay、X.25 和 SMDS 等。

（3）点到点网络（Point-to-Point），例如 PPP、HDLC 等。

（4）点到多点网络（Point-to-Multi-Point），例如运行 RARP 协议网络。

**参考答案**

（25）A　（26）C

**试题（27）**

RIPv2 是增强了的 RIP 协议，下面关于 RIPv2 的描述中，错误的是__（27）__。

（27）A. 使用广播方式来传播路由更新报文
　　B. 采用了触发更新机制来加速路由收敛
　　C. 支持可变长子网掩码和无类别域间路由
　　D. 使用经过散列的口令字来限制路由信息的传播

**试题（27）分析**

RIP 分为两个版本，RIPv1（RFC 1058，1988）是早期的路由协议，现在仍然广泛使用。RIPv1 使用目标地址为 255.255.255.255 的广播来共享路由信息，默认的路由更新周期为 30s，持有时间（Hold-Down Time）为 180s。也就是说，RIP 路由器每 30s 向它的所有邻居发送一次路由更新报文，如果在 180s 之内没有从某个邻居接收到路由更新报文，则认为该邻居已经崩溃或者其间的连接已失效。这时如果从其他邻居收到了有关同一目标的路由更新报文，则用新的路由信息替换已失效的路由表项；否则，对应的路由表项被删除。

RIP 以跳步计数（hop count）来度量路由费用，显然这不是最好的度量标准。例如，若有两条到达某个网络的连接，一个连接是经过两跳的 10M 以太网连接，一个连接是经过一跳的 64K WAN 连接，则 RIP 选取 WAN 连接作为最佳路由。在 RIP 协议中，15 跳是最大的跳数，16 跳就是不可到达网络，经过 16 跳的任何分组将被路由器丢弃。

RIPv1 是有类别的协议（classful protocol），这意味着配置 RIPv1 时必须给定 A、B 或 C 类 IP 地址和子网掩码，例如不能把子网掩码 255.255.255.0 用于 B 类网络 172.16.0.0。

对于同一个目标，RIP 路由表项中最多可以有 6 条等费用的通路，虽然默认的是 4 条。RIP 可以实现等费用通路的负载均衡（equal-cost load balancing），这种机制提供了链路冗余，以对付可能出现的连接失效，但是 RIP 不支持不等费用通路的负载均衡，这种功能出现在 IGRP 和 EIGRP 中。

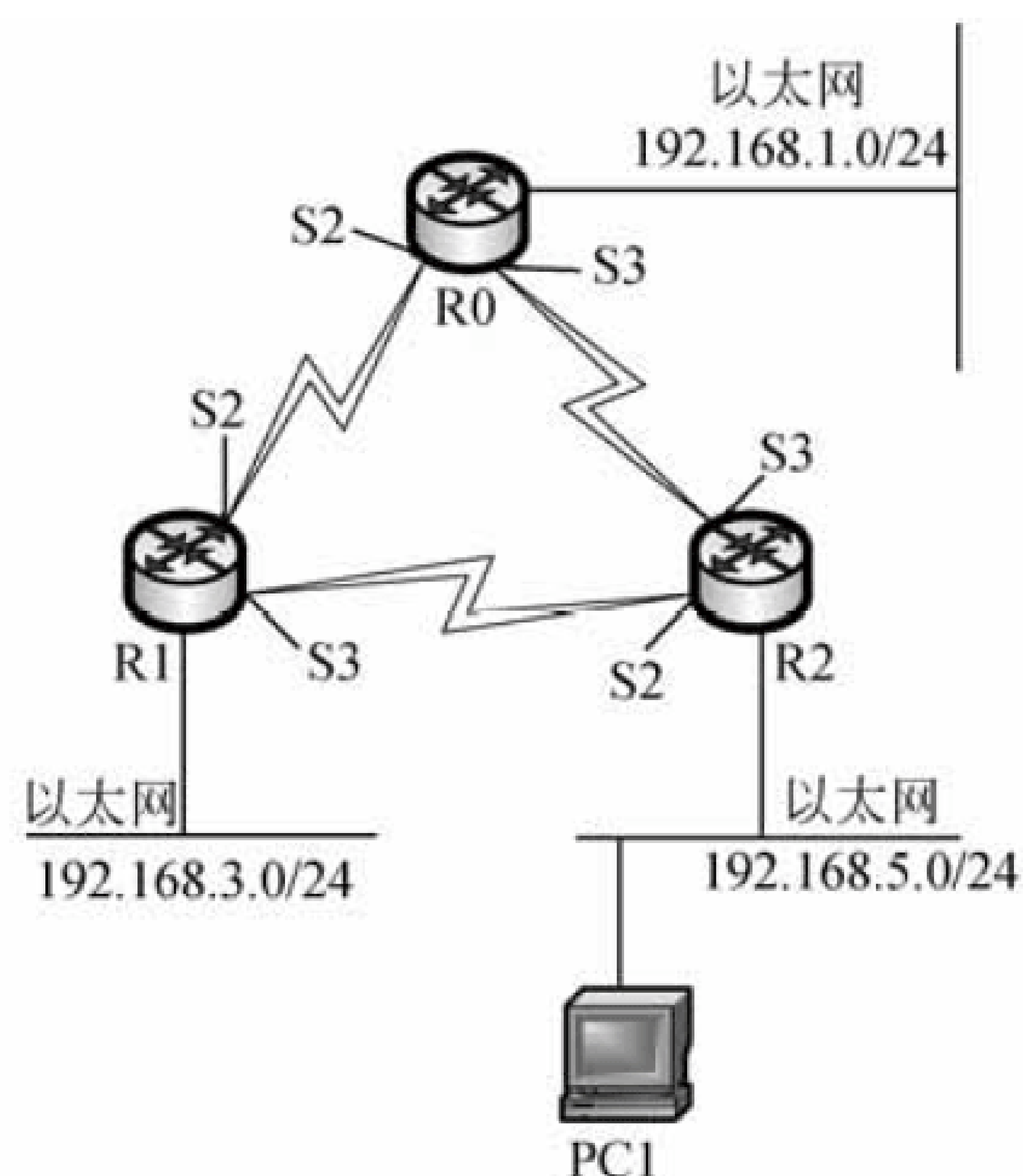
RIPv2 是增强了的 RIP 协议，基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是 RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具有伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

**参考答案**

（27）A

**试题（28）～（30）**

网络配置如下图所示：




其中某设备路由表信息如下：

C　　192.168.1.0/24 is directly connected, FastEthernet0/0

R　　192.168.3.0/24 [120/1] via 192.168.65.2, 00:00:04, Serial2/0

R　　192.168.5.0/24 [120/2] via 192.168.65.2, 00:00:04, Serial2/0

C　　192.168.65.0/24 is directly connected, Serial2/0

C　　192.168.67.0/24 is directly connected, Serial3/0

R　　192.168.69.0/24 [120/1] via 192.168.65.2, 00:00:04, Serial2/0

则该设备为__（28）__，从该设备到 PC1 经历的路径为__（29）__。路由器 R2 接口 S2 可能的 IP 地址为__（30）__。

（28）A. 路由器 R0　　B. 路由器 R1
　　　C. 路由器 R2　　D. 计算机 PC1

（29）A. R0→R2→PC1　　B. R0→R1→R2→PC1
　　　C. R1→R0→PC1　　D. R2→PC1

（30）A. 192.168.69.2　　B. 192.168.65.2
　　　C. 192.168.67.2　　D. 192.168.5.2

**试题（28）～（30）分析**

采用 show iproute 可以查看路由表信息。题中的各条命令解释如下：

（1）192.168.1.0/24 网络通过以太口 FastEthernet0/0 直连；

（2）192.168.3.0/24 网络通过串口 Serial2/0 路由可达；

（3）192.168.5.0/24 网络通过串口 Serial2/0 路由可达；

（4）192.168.65.0/24 网络通过串口 Serial2/0 直连；

（5）192.168.67.0/24 网络通过串口 Serial3/0 直连；

（6）192.168.69.0/24 网络通过串口 Serial2/0 路由可达。

依据图中拓扑信息，192.168.1.0/24 网络只和路由器 R0 直连，故空（28）选 A。

从 R0 到 PC1 所在网络 192.168.5.0/24 需经串口 Serial2/0 路由可达；串口 Serial2/0

连接的是路由器 R1，故从 R0 到 PC1 经历的路径为 R0→R1→R2→PC1，空（29）选 B。

从路由表中可以看出，192.168.1.0/24 为 R0 直连；192.168.3.0/24 为 R1 直连；192.168.5.0/24 为 R1 直连；192.168.65.0/24 直连 R0 Serial2/0 口；192.168.67.0/24 直连 R0 Serial3/0 口；S2 接口只可能属于 192.168.69.0/24 网络，故空（30）选 A。

**参考答案**

（28）A　（29）B　（30）A

**试题（31）**

下列关于 Windows 2003 中域的描述正确的是__（31）__。

（31）A. 在网络环境中所有的计算机称为一个域

B. 同一个域中可以有多个备份域控制器

C. 每个域中必须有主域控制器和备份域控制器

D. 一个域中可以有多个主域控制器

**试题（31）分析**

本题考查 Windows 域的基础知识。

域（Domain）是一个共用“目录服务数据库”的计算机和用户的集合，用于实现集中式管理。域是逻辑分组，与网络的物理拓扑无关。域中只能有一个主域控制器，但可以有零个或多个备份域控制器。

**参考答案**

（31）B

**试题（32）**

在 Windows 命令窗口中输入__（32）__命令，可见到下图所示的结果。

```
===========================================================================
Interface List
0x1 ........................MS TCP Loopback interface
0x2 ...00 16 36 33 9 b be ......Realtek RTL8139 Family PCI Fast Ethernet NIC-
数据包计划程序微型端口
===========================================================================
===========================================================================
Active Routes:
Network Destination      Netmask            Gateway            Interface    Metric
  127.0.0.0              255.0.0.0          127.0.0.1          127.0.0.1      1
  255.255.255.255        255.255.255.255    255.255.255.255    2              1
===========================================================================
Persistent Routes:
  None
```

（32）A. ipconfig /all　B. route print　C. tracert -d　D. nslookup

**试题（32）分析**

本题考查常用网络命令。

ipconfig /all 用于显示计算机中所有网络适配器（网卡、拨号连接等）的完整 TCP/IP 配置信息，如 IP 地址、子网掩码及默认网关。route print 用于查看本机路由表。tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径，-d 指定

不将 IP 地址解析到主机名称。nslookup 用于查询域名对应的 IP 地址。

**参考答案**

（32）B

**试题（33）**

Linux 操作系统中，建立动态路由需要用到文件（33）。

（33）A. /etc/hosts　　B. /etc/hostname
C. /etc/resolv.conf　　D. /etc/gateways

**试题（33）分析**

本题考查 Linux 常用配置文件。

/etc/hosts 是配置 ip 地址和其对应主机名的文件。/etc/ hostname 包含了系统的主机名称，包括完全的域名。/etc/resolv.conf 是 DNS 域名解析的配置文件。/etc/gateways 是路由表文件。

**参考答案**

（33）D

**试题（34）**

Linux 操作系统中，网络管理员可以通过修改（34）文件对 Web 服务器的端口进行配置。

（34）A. /etc/inetd.conf　　B. /etc/lilo.conf
C. /etc/httpd/conf/ httpd.conf　　D. /etc/httpd/conf/access.conf

**试题（34）分析**

本题考查 Linux 下 Web 服务器常用配置文件。

/etc/inetd.conf 是 TCP/IP 服务配置文件，在其中可以添加或删除一个服务。/etc/lilo.conf 是加载器配置文件，用于配置 Linux 的引导参数。/etc/httpd/conf/httpd.conf 为 Web 服务器主配置文件，在其中可以配置服务器所使用的端口号。/etc/httpd/conf/access.conf 包含了 Web 服务器中大部分同安全和用户访问相关的设置。

**参考答案**

（34）C

**试题（35）**

Linux 有三个查看文件的命令，若希望能够用光标上下移动来查看文件内容，应使用（35）命令。

（35）A. cat　　B. more　　C. less　　D. menu

**试题（35）分析**

本题考查 Linux 文件内容查看命令。

使用 cat、more、less 都可以查看文本内容，cat 命令一次性将文件内容全部输出，more 命令可以分页查看，less 命令可以使用光标向上或向下移动一行。menu 命令和查看文件无关。

**参考答案**

（35）C

**试题（36）**

Windows Server 2003 操作系统中，IIS 6.0 不提供下列 （36） 服务。

（36）A. Web　B. SMTP　C. POP3　D. FTP

**试题（36）分析**

本题考查 IIS 服务的基本概念。

Windows Server 2003 操作系统中，默认情况没有安装 IIS 服务，必须手工安装。 IIS 是 Windows 下架设 Web、FTP、SMTP 服务器的一套整合软件。在 IIS 中，没有提供 POP3 服务。

**参考答案**

（36）C

**试题（37）**

Windows Server 2003 操作系统中， （37） 提供了远程桌面访问。

（37）A. FTP　B. Email　C. Terminal Service　D. Http

**试题（37）分析**

本题考查网络服务的基本概念。

终端服务（Terminal Service）提供了通过作为终端仿真器工作的“瘦客户端”软件远程访问服务器桌面的能力。终端服务基本由三部分技术组成，即客户端部分、协议部分及服务器端部分。客户端和服务器通过远程桌面协议进行通信。

**参考答案**

（37）C

**试题（38）**

若在 Windows“运行”窗口中键入 （38） 命令，可以查看和修改注册表。

（38）A. CMD　B. MMC　C. AUTOEXE　D. Regedit

**试题（38）分析**

本题考查 Windows 的相关命令。

CMD 命令的作用是打开命令行终端。Microsoft 管理控制台（MMC）集成了各种工具（包括管理单元），可用来管理本地和远程计算机。Windows 中没有 AUTOEXE 命令。Regedit 提供了编辑注册表的功能。

**参考答案**

（38）D

**试题（39）**

以下关于网络安全设计原则的说法，错误的是 （39） 。

（39）A. 充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，

是设计网络安全系统的必要前提条件

B. 强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失

C. 考虑安全问题解决方案时无需考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合

D. 网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

**试题（39）分析**

网络安全设计是保证网络安全运行的基础，基本的设计原则包括强调对信息均衡、全面地进行保护的木桶原则、良好的信息安全系统必备的等级划分制度，网络信息安全的整体性原则、安全性评价与平衡原则等。在进行网络安全系统设计时应充分考虑现有网络结构以及性能价格的平衡，安全与保密系统的设计应与网络设计相结合。

**参考答案**

（39）C

**试题（40）**

在 Windows Server 2003 的 DNS 服务器中通过__（40）__操作，实现多台 Web 服务器构成集群并共享同一域名。

（40）A. 启用循环（Round Robin），添加每个 Web 服务器的主机记录

B. 禁止循环（Round Robin），启动转发器指向每个 Web 服务器

C. 启用循环（Round Robin），启动转发器指向每个 Web 服务器

D. 禁止循环（Round Robin），添加每个 Web 服务器的主机记录

**试题（40）分析**

本题考查 DNS 的基本概念。

DNS 服务器启动循环功能可以将同一域名映射到多个主机，是分享和分配网络资源的本地平衡机制。在 Windows Server 2003 的 DNS 服务器中，为了实现多台 Web 服务器构成集群并共享同一域名，需要启动 DNS 循环功能，添加每个 Web 服务器的主机记录。

**参考答案**

（40）A

**试题（41）、（42）**

廉价磁盘冗余阵列 RAID 利用冗余技术实现高可靠性，其中 RAID1 的磁盘利用率为__（41）__。如果利用 4 个盘组成 RAID3 阵列，则磁盘利用率为__（42）__。

（41）A. 25%　　B. 50%　　C. 75%　　D. 100%

（42）A. 25%　　B. 50%　　C. 75%　　D. 100%

**试题（41）、（42）分析**

本题考查廉价磁盘冗余阵列 RAID 的相关知识。

RAID 分为 0～7 这 8 个不同的冗余级别，其中 RAID0 级无冗余校验功能；RAID1

采用磁盘镜像功能，磁盘容量的利用率是 50%；RAID3 利用一台奇偶校验盘来完成容错功能。所以如果利用 4 个盘组成 RAID3 阵列，可以有 3 个盘用于有效数据，磁盘容量的利用率为 75%。

**参考答案**

（41）B　（42）C

**试题（43）**

Alice 向 Bob 发送数字签名的消息 M，则不正确的说法是__（43）__。

（43）A. Alice 可以保证 Bob 收到消息 M

B. Alice 不能否认发送过消息 M

C. Bob 不能编造或改变消息 M

D. Bob 可以验证消息 M 确实来源于 Alice

**试题（43）分析**

本题考查数字签名的相关概念。

数字签名设计为发送者不可否认、接收者可以验证但不能编造或篡改。所以选项 B、C 和 D 都是正确的。选项 A 显然是错误的。

**参考答案**

（43）A

**试题（44）**

安全散列算法 SHA-1 产生的摘要的位数是__（44）__。

（44）A. 64　B. 128　C. 160　D. 256

**试题（44）分析**

本题考查安全散列算法 SHA-1 的基础知识。

安全散列算法 SHA-1 是 SHA 的改进版本，此算法以最大长度不超过 $2^{64}$ 位的消息为输入，生成 160 位的消息摘要输出，用 512 为块来处理输入。

**参考答案**

（44）C

**试题（45）**

在 X.509 标准中，不包含在数字证书中的数据域是__（45）__。

（45）A. 序列号　B. 签名算法

C. 认证机构的签名　D. 私钥

**试题（45）分析**

本题考查数字证书的基础知识。

数字证书中包含用户的公钥，而用户的私钥只能被用户拥有。所以选项 D 是不可能包含在数字证书中的。

**参考答案**

（45）D

**试题（46）、（47）**

两个公司希望通过 Internet 传输大量敏感数据，从信息源到目的地之间的传输数据以密文形式出现，而且不希望由于在传输节点使用特殊的安全单元而增加开支，最合适的加密方式是__（46）__，使用会话密钥算法效率最高的是__（47）__。

（46）A. 链路加密　B. 节点加密　C. 端-端加密　D. 混合加密

（47）A. RSA　B. RC-5　C. MD5　D. ECC

**试题（46）、（47）分析**

通过 Internet 传输数据，报文在路由器间依据路由选择算法进行转发，所经过的路径并不唯一，故采用链路加密难以实现；节点加密开支过大；混合加密结合多种方式，也不符合题意；端-端加密在发送端与接收端之间进行加解密，是最合适的加密方式。在传输过程中采用对称密钥比非对称密钥效率要高，故选择 RC-5。

**参考答案**

（46）C　（47）B

**试题（48）**

包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括__（48）__。

（48）A. 源地址　B. 目的地址　C. 协议　D. 有效载荷

**试题（48）分析**

本题考查包过滤防火墙的相关知识。

防火墙的基本功能是包过滤，能对进出防火墙的数据包包头（包括源地址、目的地址和协议）进行分析处理，但对于数据包的有效载荷一般无法分析处理。所以答案是 D。

**参考答案**

（48）D

**试题（49）**

下面关于 ARP 木马的描述中，错误的是__（49）__。

（49）A. ARP 木马利用 ARP 协议漏洞实施破坏

B. ARP 木马发作时可导致网络不稳定甚至瘫痪

C. ARP 木马破坏网络的物理连接

D. ARP 木马把虚假的网关 MAC 地址发送给受害主机

**试题（49）分析**

本题考查计算机病毒的相关知识。

ARP 木马的工作原理是利用 ARP 协议漏洞，把虚假的网关 MAC 地址发送给受害主机，造成局域网内出现大量的 ARP 消息从而造成网络拥塞。但并没有破坏网络的物理连

通性。所以选项 C 是错误的。

**参考答案**

（49）C

**试题（50）**

下面几个网络管理工具的描述中，错误的是___（50）___。

（50）A. netstat 可用于显示 IP、TCP、UDP、ICMP 等协议的统计数据
B. sniffer 能够使网络接口处于杂收模式，从而可截获网络上传输的分组
C. winipcfg 采用 MS-DOS 工作方式显示网络适配器和主机的有关信息
D. tracert 可以发现数据包到达目标主机所经过的路由器和到达时间

**试题（50）分析**

本题考查网络管理工具。

其中，netstat 可用于显示 IP、TCP、UDP、ICMP 等协议的统计数据；sniffer 能够使网络接口处于杂收模式，从而可截获网络上传输的分组；winipcfg 在 Windows 中显示网络适配器和主机的有关信息；tracert 可以发现数据包到达目标主机所经过的路由器和到达时间。

**参考答案**

（50）C

**试题（51）**

一个网络的地址为 172.16.7.128/26，则该网络的广播地址是___（51）___。

（51）A. 172.16.7.255　　B. 172.16.7.129
C. 172 .16.7.191　　D. 172.16.7.252

**试题（51）分析**

IP 地址分为网络地址和主机地址两部分，一个网络的广播地址是将其主机地址部分置为全 1。地址 172.16.7.128/26 的二进制形式为 10101100.00010000.00000111.10**000000**，则该网络的广播地址是 10101100.00010000.00000111.10**111111**，即 172.16.7.191。

**参考答案**

（51）C

**试题（52）**

使用 CIDR 技术把 4 个 C 类网络 192.24.12.0/24、192.24.13.0/24、192.24.14.0/24 和 192.24.15.0/24 汇聚成一个超网，得到的地址是___（52）___。

（52）A. 192.24.8.0/22　　B. 192.24.12.0/22
C. 192.24.8.0/21　　D. 192.24.12.0/21

**试题（52）分析**

CIDR 技术是把小的网络汇聚成大的超网。这里的 4 个网络地址的二进制表示如下。

192.24.12.0/24 的二进制表示为：　**11000000 00011000 00001100** 00000000

192.24.13.0/24 的二进制表示为： **11000000 00011000 00001101** 00000000

192.24.14.0/24 的二进制表示为： **11000000 00011000 00001110** 00000000

192.24.15.0/24 的二进制表示为： **11000000 00011000 00001111** 00000000

可以看出，汇聚后的网络地址为 **11000000 00011000 000011**00 00000000，即 192.24.12.0/22。

**参考答案**

（52）B

**试题（53）**

某公司网络的地址是 133.10.128.0/17，被划分成 16 个子网，下面的选项中不属于这 16 个子网的地址是__（53）__。

（53）A. 133.10.136.0/21 B. 133.10.162.0/21

C. 133.10.208.0/21 D. 133.10.224.0/21

**试题（53）分析**

地址 133.10.128.0/17 的二进制表示为：

**10000101.00001010.1**0000000.00000000

将其划分为 16 个子网，则各个子网的地址为：

10000101.00001010.1**0000**000.00000000——133.10.128.0/21

10000101.00001010.1**0001**000.00000000——133.10.136.0/21

10000101.00001010.1**0010**000.00000000——133.10.144.0/21

10000101.00001010.1**0011**000.00000000——133.10.152.0/21

10000101.00001010.1**0100**000.00000000——133.10.160.0/21

10000101.00001010.1**0101**000.00000000——133.10.168.0/21

10000101.00001010.1**0110**000.00000000——133.10.176.0/21

10000101.00001010.1**0111**000.00000000——133.10.184.0/21

10000101.00001010.1**1000**000.00000000——133.10.192.0/21

10000101.00001010.1**1001**000.00000000——133.10.200.0/21

10000101.00001010.1**1010**000.00000000——133.10.208.0/21

10000101.00001010.1**1011**000.00000000——133.10.216.0/21

10000101.00001010.1**1100**000.00000000——133.10.224.0/21

10000101.00001010.1**1101**000.00000000——133.10.232.0/21

10000101.00001010.1**1110**000.00000000——133.10.240.0/21

10000101.00001010.1**1111**000.00000000——133.10.248.0/21

可以看出，以上 16 个网络地址的第三个字节都能被 8 整除，而答案 B 中的 162 不能被 8 整除。

**参考答案**

（53）B

**试题（54）**

以下地址中不属于网络 100.10.96.0/20 的主机地址是__（54）__。

（54）A. 100.10.111.17　　B. 100.10.104.16

C. 100.10.101.15　　D. 100.10.112.18

**试题（54）分析**

地址 100.10.111.17 的二进制形式为：　01100100.00001010.01101111.00010001

地址 100.10.104.16 的二进制形式为：　01100100.00001010.01101000.00010000

地址 100.10.101.15 的二进制形式为：　01100100.00001010.01100101.00001111

地址 100.10.112.18 的二进制形式为：　01100100.00001010.01110000.00010010

而地址 100.10.96.0/20 的二进制形式为：　**01100100.00001010.0110**0000.00000000

只有答案 D 不能与其匹配。

**参考答案**

（54）D

**试题（55）、（56）**

自动专用 IP 地址（Automatic Private IP Address，APIPA）是 IANA（Internet Assigned Numbers Authority）保留的一个地址块，它的地址范围是__（55）__。当__（56）__时，使用 APIPA。

（55）A．A 类地址块 10.254.0.0～10.254.255.255

B．类地址块 100.254.0.0～100.254.255.255

C．类地址块 168.254.0.0～168.254.255.255

D．B 类地址块 169.254.0.0～169.254.255.255

（56）A．通信对方要求使用 APIPA 地址

B．由于网络故障而找不到 DHCP 服务器

C．客户机配置中开启了 APIPA 功能

D．DHCP 服务器分配的租约到期

**试题（55）、（56）分析**

自动专用 IP 地址（Automatic Private IP Address，APIPA）是当客户端无法从 DHCP 服务器中获得 IP 地址时自动配置的地址。IPv4 地址前缀 169.254/16 已经被 IANA 注册为 APIPA 专用（RFC 3927）。

当网络中的 DHCP 服务器失效，或者由于网络故障而找不到 DHCP 服务器时，这个功能开始生效，使得客户端可以在一个小型局域网中运行，与其他自动或手工获得 APIPA 地址的计算机进行通信。其实 APIPA 的主要用途是为了移动计算使用的，两个笔记本式计算机用户之间可以通过 APIPA 地址直接通信，而不需要其他网络连接的支持。

**参考答案**

（55）D （56）B

**试题（57）**

VLAN中继协议（VTP）用于在大型交换网络中简化VLAN的管理。按照VTP协议，交换机的运行模式分为3种：服务器、客户机和透明模式。下面关于VTP协议的描述中，错误的是__（57）__。

（57）A. 交换机在服务器模式下能创建、添加、删除和修改VLAN配置

B. 一个管理域中只能有一个服务器

C. 在透明模式下可以进行VLAN配置，但不能向其他交换机传播配置信息

D. 交换机在客户机模式下不允许创建、修改或删除VLAN

**试题（57）分析**

VLAN中继协议（VLAN Trunking Protocol，VTP）是Cisco公司的专利协议，用于在大型交换网络中简化VLAN的管理。VTP协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享VLAN信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享VLAN信息。通过VTP协议，可以在一台交换机上配置所有的VLAN，配置信息通过VTP报文可以传播到管理域中的所有交换机。

按照VTP协议，交换机的运行模式分为3种：

（1）服务器模式（Server）。交换机在此模式下能创建、添加、删除和修改VLAN配置，并从中继端口发出VTP组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

（2）客户机模式（Client）。交换机在此模式下不允许创建、修改或删除VLAN，但可以监听本管理域中其他交换机的VTP组播信息，并据此修改自己的VLAN配置。

（3）透明模式（Transparent）。交换机在此模式下可以进行VLAN配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发VTP帧，但是并不能据此更新自己的VLAN配置，只是起到通路的作用。

VTP协议的优点有：

- 提供通过一个交换机在整个管理域中配置VLAN的方法；
- 提供跨不同介质类型（如ATM、FDDI和以太网）配置VLAN的方法；
- 提供跟踪和监视VLAN配置的方法；
- 保持VLAN配置的一致性。

**参考答案**

（57）B

**试题（58）**

新交换机出厂时的默认配置是__（58）__。

（58）A. 预配置为VLAN 1，VTP模式为服务器

B. 预配置为 VLAN 1，VTP 模式为客户机
C. 预配置为 VLAN 0，VTP 模式为服务器
D. 预配置为 VLAN 0，VTP 模式为客户机

**试题（58）分析**

新交换机出厂时的预配置为 VLAN 1，VTP 模式为服务器。

**参考答案**

（58）A

**试题（59）**

在生成树协议（STP）IEEE 802.1d 中，根据 （59） 来选择根交换机。

（59）A. 最小的 MAC 地址　　B. 最大的 MAC 地址
C. 最小的交换机 ID　　D. 最大的交换机 ID

**试题（59）分析**

生成树协议（Spanning Tree Protocol，STP）是交换式以太网中的重要技术，其目的是在交换机之间存在冗余连接的情况下避免网络中出现环路，实现网络的高可靠性。STP 原来是 DEC 公司开发的协议，IEEE 增强了它的功能，颁布了 802.1d 标准。这两种实现不兼容，Cisco 交换机默认支持 802.1d 协议。

802.1d 定义了交换机之间交换的网桥协议数据单元 BPDU（如下图所示），其中包含了交换网络的拓扑结构信息，例如交换机（或网桥）标识符 BID、链路性质和根交换机标识符（Rood BID）等。

| Protocol ID (2) | Version (1) | Type (1) | Flags (1) | Rood BID (8) | Root Path (4) |
|---|---|---|---|---|---|
| Sender BID (8) | Port ID (2) | M-Age (2) | Max Age (2) | Hello (2) | FD (2 Bytes) |

网桥协议数据单元示意图

当交换网络中有多个 VLAN 时，一个交换机在每个 VLAN 中有不同的 BID，每个 VLAN 运行 STP 协议的一个实例，每个 VLAN 都有它自己的根交换机，各个 VLAN 的根交换机可以相同，也可以不同。在每个 VLAN 中，由 STP 协议确定根交换机，决定哪些端口处于转发状态，哪些端口处于阻塞状态，以免引起 VLAN 内部的环路。

按照 802.1d 定义的生成树算法，每个网桥有唯一的 MAC 地址和唯一的优先级，地址和优先级构成网桥的标识符 BID（8 字节）。根桥是作为生成树根的网桥，通常选择 BID 最小的网桥作为根桥。其他网桥选择到达根桥费用最小的通路作为根通路（Root Path），与根桥连接的端口称为根端口。互相连接的每个 LAN 都有一个指定桥，这是在该 LAN 上能提供最小费用根通路的网桥。指定桥连接 LAN 的端口叫作指定端口。按照以上算法，直接连接两个 LAN 的网桥中只能有一个作为指定桥，其他都从生成树中删除掉，这就排除了两个 LAN 之间的任何环路。同理，以上算法也排除了多个 LAN 之间的环路，但保持了连通性。

由于 802.1d 协议的生成树算法收敛速度比较慢，可能达到 30～50s，对于某些实时应用（例如 VoIP）这是不能容忍的，因此 IEEE 把 Cisco 交换机的一些扩展特性融入原来的 802.1d 中，颁布了收敛速度更快的快速生成树协议（Rapid Spanning Tree Protocol，RSTP）802.1w，提供了交换机、交换机端口或整个网络的快速故障恢复功能。

**参考答案**

（59）C

**试题（60）**

在快速以太网物理层标准中，使用两对 5 类无屏蔽双绞线的是＿（60）＿。

（60）A. 100Base-TX　　B. 100Base-FX
　　C. 100Base-T4　　D. 100Base-T2

**试题（60）分析**

1995 年，100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布，这是基于 10Base-T 和 10Base-F 技术、在基本布线系统不变的情况下开发的高速局域网标准。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为 62.5μm，包层直径为 125μm；单模光纤的芯线直径为 8μm，包层直径也是 125μm。

**快速以太网物理层规范**

| 标　准 | 传 输 介 质 | 特 性 阻 抗 | 最 大 段 长 |
|---|---|---|---|
| 100Base-TX | 2 对 5 类 UTP | 100Ω | 100m |
| | 2 对 STP | 150Ω | |
| 100Base-FX | 一对多模光纤 MMF | 62.5/125μm | 2km |
| | 一对单模光纤 SMF | 8/125μm | 40km |
| 100Base-T4 | 4 对 3 类 UTP | 100Ω | 100m |
| 100Base-T2 | 2 对 3 类 UTP | 100Ω | 100m |

**参考答案**

（60）A

**试题（61）、（62）**

在 Windows 系统中，所谓“持久路由”就是＿（61）＿。要添加一条到达目标 10.40.0.0/16 的持久路由，下一跃点地址为 10.27.0.1，则在 DOS 窗口中键入命令＿（62）＿。

（61）A. 保存在注册表中的路由　　B. 在默认情况下系统自动添加的路由
　　C. 一条默认的静态路由　　D. 不能被删除的路由

（62）A. route -s add 10.40.0.0 mask 255.255.0.0 10.27.0.1
　　B. route -p add 10.27.0.1 10.40.0.0 mask 255.255.0.0
　　C. route -p add 10.40.0.0 mask 255.255.0.0 10.27.0.1
　　D. route -s add 10.27.0.1 10.40.0.0 mask 255.255.0.0

**试题（61）、（62）分析**

Windows Server 2003 的路由类型有 5 种，见下表。当 Windows 服务器收到一个 IP 数据包时，查找路由的优先次序是主机路由、网络路由、默认路由。

**路由类型**

| 路 由 类 型 | 说　明 |
|---|---|
| 直连网络 ID（Directly attached network ID） | 用于直接连接的网络，Interface（或 next hop）可以为空 |
| 远程网络 ID（Remote network ID） | 用于不直接连接的网络，可以通过其他路由器到达这种网络，Interface 字段是本地路由器的 IP 地址 |
| 主机路由（Host route） | 到达特定主机的路由，子网掩码为 255.255.255.255 |
| 默认路由（Default route） | 无法找到确定路由时使用的路由，目标网络和网络掩码都是 0.0.0.0 |
| 持久路由（Persistent route） | 利用 route add -p 命令添加的表项，每次初始化时，这种路由都会加入 Windows 的注册表中，同时加入路由表 |

持久路由（Persistent route）是利用 route add -p 命令添加的表项，每次初始化时，这种路由都会加入 Windows 的注册表中，同时加入路由表。

Route 命令的功能是显示和修改本地的 IP 路由表，如果不带参数，则给出帮助信息。Route 命令的语法如下：

route[-f] [-p] [*Command* [*Destination*] [*mask Netmask*] [*Gateway*] [metric *Metric*]] [*if Interface*]]

对以上参数解释如下：

- -f

删除路由表中的网络路由（子网掩码不是 255.255.255.255）、本地环路路由（目标地址为 127.0.0.0，子网掩码为 255.0.0.0）和组播路由（目标地址为 224.0.0.0，子网掩码为 240.0.0.0）。如果与其他命令（例如 add、change 或 delete）联合使用，在运行这个命令前先清除路由表。

- -p

与 add 命令联合使用时，一条路由被添加到注册表中，当 TCP/IP 协议启动时，用于初始化路由表。在默认情况下，系统重新启动时不保留添加的路由。与 print 命令联合使用时则显示持久路由列表。对于其他命令，这个参数被忽略。持久路由保存在注册表中的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Persistent Routes 位置。

- *Command*

表示要运行的命令，可用的命令有 add（添加路由）、change（修改路由）、delete（删

除路由）和 print（显式路由表）。

- *Destination*

说明目标地址，可以是网络地址（IP 地址中对应主机的位都是 0）、主机地址或默认路由（0.0.0.0）。

- *mask Netmask*

说明了目标地址对应的子网掩码。网络地址的子网掩码依据网络的大小而变化，主机地址的子网掩码为 255.255.255.255，默认路由的子网掩码为 0.0.0.0。如果忽略了这个参数，默认的子网掩码为 255.255.255.255。由于在路由寻址中具有关键作用，因此目标地址不能特异于对应的子网掩码。换言之，如果子网掩码的某个位是 0，则目标地址的对应位不能为 1。

- *Gateway*

说明下一跃点的 IP 地址。对于本地连接的子网，网关地址是本地子网中分配给接口的 IP 地址；对于远程路由，网关地址是相邻路由器中直接连接的 IP 地址。

- *metric Metric*

说明路由度量值（1～9999）。通常选择度量值最小的路由。度量值可以根据跃点数、链路速率、通路可靠性、通路的吞吐率以及管理属性等参数确定。

- *if Interface*

说明接口的索引。使用 route print 命令可以显示接口索引列表。接口索引可以使用十进制数或十六进制数表示。如果忽略 if 参数，接口索引根据网关地址确定。

**参考答案**

（61）A　（62）C

**试题（63）**

访问控制列表（ACL）分为标准和扩展两种。下面关于 ACL 的描述中，错误的是__（63）__。

（63）A. 标准 ACL 可以根据分组中的 IP 源地址进行过滤

B. 扩展 ACL 可以根据分组中的 IP 目标地址进行过滤

C. 标准 ACL 可以根据分组中的 IP 目标地址进行过滤

D. 扩展 ACL 可以根据不同的上层协议信息进行过滤

**试题（63）分析**

访问控制列表（ACL）根据源地址、目标地址、源端口或目标端口等协议信息对数据包进行过滤，从而达到访问控制的目的。ACL 分为标准的和扩展的两种类型。标准 ACL 只能根据分组中的 IP 源地址进行过滤，例如可以允许或拒绝来自某个源设备的所有通信。扩展 ACL 不但可以根据源地址或目标地址进行过滤，还可以根据不同的上层

协议和协议信息进行过滤。例如，可以对 PC 与远程服务器的 Telnet 会话进行过滤。两种 ACL 过滤功能的区别如下表所示。

**CL 过滤信息**

| 过 滤 信 息 | 标准 ACL | 扩展 ACL |
|---|---|---|
| 源地址 | √ | √ |
| 目标地址 | × | √ |
| 上层协议 | × | √ |
| 协议信息 | × | √ |

**参考答案**

（63）C

**试题（64）**

如果要测试目标 10.0.99.221 的连通性并进行反向名字解析，则在 DoS 窗口中键入命令＿（64）＿。

（64）A. ping -a 10.0.99.221　　B. ping -n 10.0.99.221

C. ping -r 10.0.99.221　　D. ping -j 10.0.99.221

**试题（64）分析**

Ping 命令通过发送 ICMP 回声请求报文来检验与另外一个计算机的连接。这是一个用于排除连接故障的测试命令，如果不带参数则显示帮助信息。Ping 命令的语法如下：

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count]
[-s Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]
```

对以上命令参数解释如下：

- -t

持续发送回声请求直至按 Ctrl+Break 或 Ctrl+C 快捷键被中断，前者显示统计信息，后者不显示统计信息。

- -a

用 IP 地址表示目标，进行反向名字解析，如果命令执行成功，则显示对应的主机名。

- -n Count

说明发送回声请求的次数，默认为 4 次。

- -l Size

说明了回声请求报文的字节数，默认是 32，最大为 65 527。

- -f

在 IP 头中设置不分段标志，用于测试通路上传输的最大报文长度。

- -i *TTL*

说明 IP 头中 TTL 字段的值，通常取主机的 TTL 值，对于 Windows XP 主机，这个值是 128，最大为 255。

- -v *TOS*

说明了 IP 头中 TOS（Type of Service）字段的值，默认是 0。

- -r *Count*

在 IP 头中添加路由记录选项，Count 表示源和目标之间的跃点数，其值在 1～9 之间。

- -s *Count*

在 IP 头中添加时间戳（timestamp）选项，用于记录达到每一跃点的时间，Count 的值在 1～4 之间。

- *-j HostList*

在 IP 头中使用松散源路由选项，HostList 指明中间节点（路由器）的地址或名字，最多 9 个，用空格分开。

- -k HostList

在 IP 头中使用严格源路由选项，HostList 指明中间节点（路由器）的地址或名字，最多 9 个，用空格分开。

- -w Timeout

指明等待回声响应的时间（μs），如果响应超时，则显示出错信息“Request timed out”，默认超时间隔为 4s。

- TargetName

用 IP 地址或主机名表示目标设备。

**参考答案**

（64）A

**试题（65）**

在 IEEE 802.11 标准中使用了扩频通信技术，下面选项中有关扩频通信技术说法正确的是__（65）__。

（65）A. 扩频技术是一种带宽很宽的红外线通信技术

B. 扩频技术就是用伪随机序列对代表数据的模拟信号进行调制

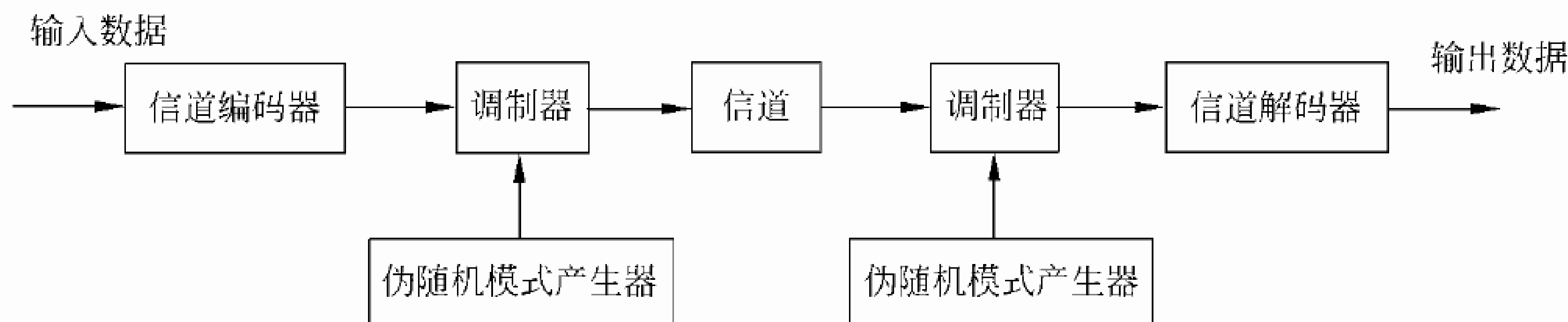
C. 扩频通信系统的带宽随着数据速率的提高而不断扩大

D. 扩频技术就是扩大了频率许可证的使用范围

**试题（65）分析**

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（Frequency Hopping Spread Spectrum，FHSS），更新的版本是直接序列扩展频谱（Direct Sequence Spread Spectrum，DSSS）。

下图表示了各种扩展频谱系统的共同特点。输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号，再用一个伪随机序列对这个信号进行调制。调制的结果是大大拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后再进入信道解码器来恢复数据。




扩展频谱通信系统的模型

伪随机序列由一个使用初值（称为种子 seed）的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计得好，得到的序列能够通过各种随机性测试，这就是被叫作伪随机序列的原因。重要的是，除非你知道算法与种子，否则预测序列是不可能的。因此，只有与发送器共享同一伪随机序列的接收器才能成功地对信号进行解码。

**参考答案**

（65）B

**试题（66）**

下面关于 WLAN 安全标准 IEEE 802.11i 的描述中，错误的是＿（66）＿。

（66）A. 采用了高级加密标准 AES

B. 定义了新的密钥交换协议 TKIP

C. 采用 802.1x 实现访问控制

D. 提供的加密方式为有线等价协议 WEP

**试题（66）分析**

原来的 IEEE 802.11 标准提供的加密方式是有线等价协议（Wired Equivalency Protocol，WEP），WEP 包括共享密钥认证和数据加密两个过程。共享密钥认证使得没有 WEP 密钥的用户无法访问网络，而加密则要求所有数据必须用密文传输。

认证采用了标准的询问和响应帧格式。执行过程中，AP 根据 RC 4 算法运用共享密钥对 128 字节的随机序列进行加密后作为询问帧发给用户，用户将收到的询问帧进行解密后以明文形式响应 AP，AP 将明文与原始随机序列进行比较，如果两者一致，则通过认证。

2004 年 6 月公布的 IEEE 802.11i 标准是对 WEP 协议的改进，为无线局域网提供了全新的安全技术。802.11i 定义了新的密钥交换协议（Temporal Key Integrity Protocol，

TKIP）和高级加密标准（Advanced Encryption Standard，AES）。TKIP 提供了报文完整性检查，每个数据包使用不同的混合密钥（per-packet key mixing），每次建立连接时生成一个新的基本密钥（re-keying），这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而弥补了 WEP 协议的安全隐患。另外，IEEE 802.11 还采用 802.1x 实现访问控制，根据用户端的 MAC 地址进行认证，从而防止了非法访问。

**参考答案**

（66）D

**试题（67）**

安全审计是保障计算机系统安全的重要手段，其作用不包括（67）。

（67）A. 重现入侵者的操作过程

B. 发现计算机系统的滥用情况

C. 根据系统运行的日志，发现潜在的安全漏洞

D. 保证可信计算机系统内部信息不外泄

**试题（67）分析**

安全审计包括识别、记录、存储、分析与安全相关行为的信息，审计记录用于检查与安全相关的活动和负责人。安全审计系统就是根据一定的安全策略记录和分析历史操作事件及数据，发现能够改进系统运行性能和系统安全的地方。安全审计的作用包括对潜在的攻击者起到震慑或警告的作用、检测和制止对安全系统的入侵、发现计算机的滥用情况、为系统管理员提供系统运行的日志，从而能发现系统入侵行为和潜在的漏洞及对已经发生的系统攻击行为提供有效的追究证据。安全审计系统通常有一个统一的集中管理平台，支持集中管理，并支持对日志代理、安全审计中心、日志、数据库的集中管理，并具有事件响应机制和联动机制。

**参考答案**

（67）D

**试题（68）**

网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（68）。

（68）A. 多重安全网关　　B. 防火墙

C. VLAN 隔离　　D. 物理隔离

**试题（68）分析**

网络隔离（Network Isolation）技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。有多种形式的网络隔离，如物理隔离、协议隔离和 VPN 隔离等。无论采用什么形式的网络隔离，其实质都是数据或信息的隔离。网络隔离的重点是物理隔离。物理隔离的一个特征，就是内网与外网永不连接，内网和外网在同一时间最多只有一个同隔离设备建立非 TCP/IP

协议的数据连接。

**参考答案**

（68）D

**试题（69）**

下列有关网络设备选型原则中，不正确的是__（69）__。

（69）A. 所有网络设备尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持、价格等方面都更有优势

B. 在网络的层次结构中，主干设备选择可以不考虑扩展性需求

C. 尽可能保留并延长用户对原有网络设备的投资，减少在资金投入上的浪费

D. 选择性能价格比高、质量过硬的产品，使资金的投入产出达到最大值

**试题（69）分析**

本题考查网络设备选型的基本原理。

所有网络设备尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持、价格等方面都更有优势。在网络的层次结构中，主干设备选择应预留一定的能力，以便将来扩展，而低端设备则够用即可。同时，应尽可能保留并延长用户对原有网络设备的投资，使资金的投入产出达到最大值，能以较低的成本、较少的人员投入来维持系统运转。网络系统应具有较高的可靠性。全系统的可靠性主要体现在网络设备的可靠性。

**参考答案**

（69）B

**试题（70）**

在层次化网络设计中，__（70）__不是分布层/接入层交换机的选型策略。

（70）A. 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便由于信息点的增加而进行扩容

B. 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单

C. 具备一定的网络服务质量和控制能力以及端到端的 QoS

D. 具备高速的数据转发能力

**试题（70）分析**

本题考查层次化网络中网络设备选型的基本原理。

分布层/接入层交换机也称外围交换机或边缘交换机，一般都属于可堆叠，可扩充式固定端口交换机。在大中型网络中它用来构成多层次的结构灵活的用户接入网络，在中小型网络中它也可能用来构成网络骨干交换设备，应具备下列要求：

（1）灵活性。提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便由于信息点的增加而进行扩容。

（2）高性能。作为大型网络的二级交换设备，应支持千兆/百兆高速上连（最好支持 FEC/GEC），以及同级设备堆叠，当然还要注意与核心交换机品牌的一致性；如果用作小型网络的中央交换机，要求具有较高的背板带宽和三层交换能力等。

（3）在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单。

（4）具备一定的网络服务质量和控制能力以及端到端的 QoS。

（5）如果用于跨地区企业分支部门通过公网进行远程上联的交换机，还应支持虚拟专网 VPN 标准协议。

（6）支持多级别网络管理。

**参考答案**

（70）D

**试题（71）～（75）**

The Border Gateway Protocol (BGP) is an interautonomous system __(71)__ protocol. The primary function of a BGP speaking system is to exchange network __(72)__ information with other BGP system. This network reachability information includes information on the list of Autonomous System (ASs) that reachability information traverses. BGP-4 provides a new set of mechanisms for supporting __(73)__ interdomain routing. These mechanisms include support for advertising an IP __(74)__ and eliminate the concept of network class within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including __(75)__ of AS paths. These changes provide support for the proposed supernettting scheme.

（71）A. connecting　B. resolving　C. routing　D. supernettting

（72）A. secubility　B. reachability　C. capability　D. reliability

（73）A. answerless　B. connectionless　C. confirmless　D. classless

（74）A. prefix　B. suffix　C. infix　D. reflex

（75）A. reservation　B. relation　C. aggregation　D. connection

**参考译文**

边界网关协议 BGP 是自治系统间的路由协议。BGP 发布系统的基本功能就是与其他 BGP 系统交换网络可到达性信息。这种网络可到达性信息包含了可到达性信息穿越的自治系统的列表。BGP-4 提供了一系列新的机制来支持无类别的域间路由。这些机制包括支持发布 IP 前缀，从而在 BGP 中排除了网络类别的概念。BGP-4 也引入了路由聚合机制，包括 AS 通路的聚合。这些改变提供了对提议的超网方案的支持。

**参考答案**

（71）C　（72）B　（73）D　（74）A　（75）C

# 第 2 章　2009 上半年网络工程师下午试题分析与解答

**试题一（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司有 1 个总部和两个分部，各个部门都有自己的局域网。该公司申请了 4 个 C 类 IP 地址块 202.114.10.0/24～202.114.13.0/24。公司各部门通过帧中继网络进行互联，网络拓扑结构如图 1-1 所示。

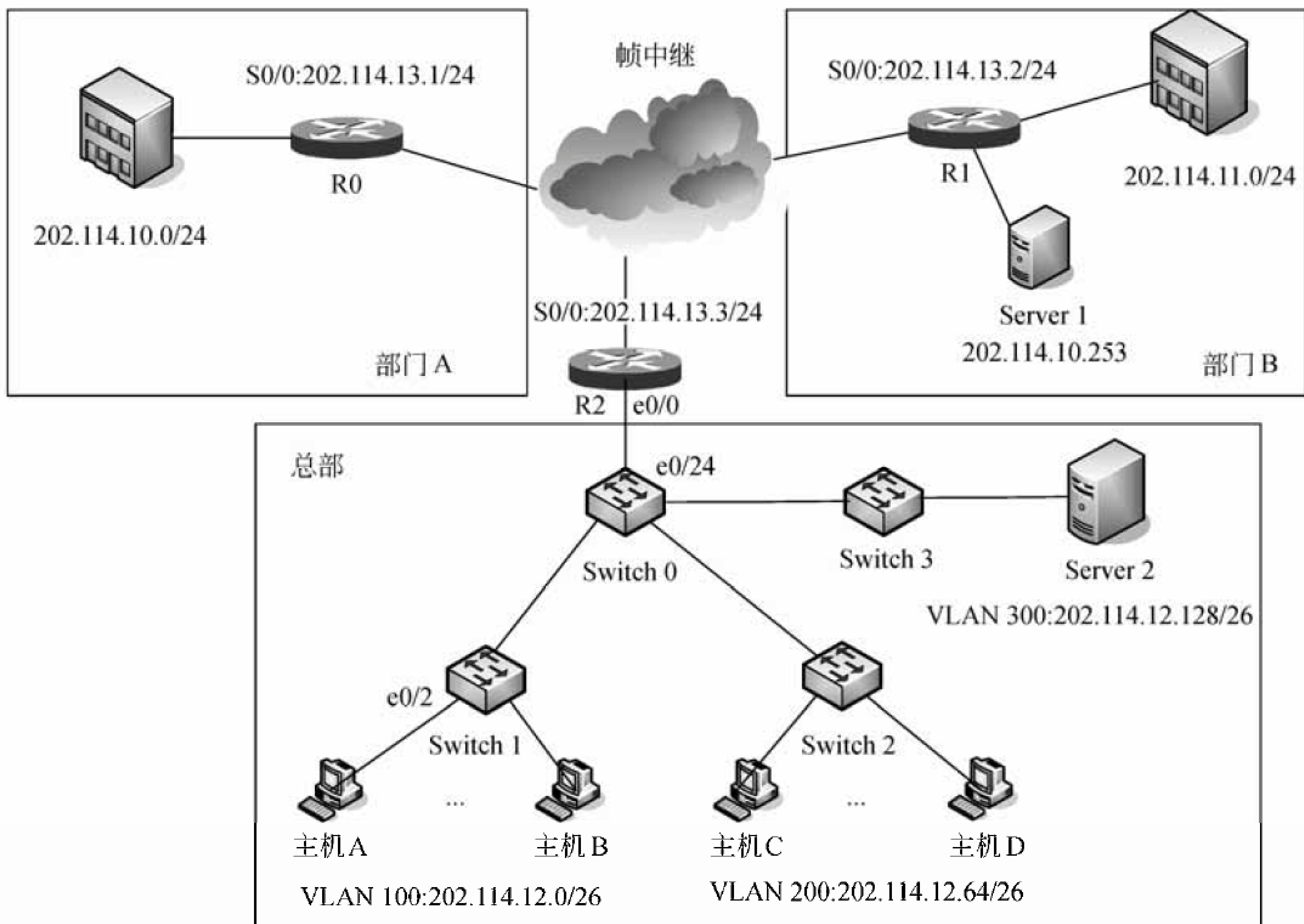



图 1-1

**【问题 1】（4 分）**

请根据图 1-1 完成 R0 路由器的配置：

```
R0 (config) #interface s0/0                          (进入串口配置模式)
```

```
R0 (config-if) # ip address 202.114.13.1 ___(1)___     (设置IP地址和掩码)
R0 (config) # encapsulation ___(2)___                  (设置串口工作模式)
```

【问题2】(5分)

Switch0、Switch1、Switch2和Switch3均为二层交换机。总部拥有的IP地址块为202.114.12.0/24。Switch0的端口e0/24与路由器R2的端口e0/0相连，请根据图1-1完成路由器R2及Switch0的配置。

```
R2 (config) #interface fastethernet 0/0.1
R2 (config-subif) #encapsulation dot1q ___(3)___
R2 (config-subif) #ip address 202.114.12.1 255.255.255.192
R2 (config-subif) #no shutdown
R2 (config-subif) #exit
R2 (config) #interface fastethernet 0/0.2
R2 (config-subif) #encapsulation dot1q ___(4)___
R2 (config-subif) #ip address 202.114.12.65 255.255.255.192
R2 (config-subif) #no shutdown
R2 (config-subif) #exit
R2 (config) #interface fastethernet 0/0.3
R2 (config-subif) #encapsulation dot1q ___(5)___
R2 (config-subif) #ip address 202.114.12.129 255.255.255.192
R2 (config-subif) #no shutdown
R2 (config-subif) #exit
R2 (config) #interface fastether0/0
R2 (config-if) #no shutdown

Switch0 (config) #interface f0/24
Switch0 (config-if) # switchport mode ___(6)___
Switch0 (config-if) #switchport trunk encapsulation ___(7)___
Switch0 (config-if) # switchport trunk allowed all
Switch0 (config-if) #exit
```

【问题3】(3分)

若主机A与Switch1的e0/2端口相连，请完成Switch1相应端口设置。

```
Switch1 (config) #interface e0/2
Switch1 (config-if) #___(8)___        (设置端口为接入链路模式)
Switch1 (config-if) #___(9)___        (把e0/2分配给VLAN 100)
Switch1 (config-if) #exit
```

若主机A与主机D通信，请填写主机A与D之间的数据转发顺序。

主机 A→ ___（10）___→主机 D。

（10）备选答案：

A．Switch1→Switch0→R2（s0/0）→Switch0→Switch2

B．Switch1→Switch0→R2（e0/0）→Switch0→Switch2

C．Switch1→Switch0→R2（e0/0）→R2（s0/0）→R2（e0/0）→Switch0→Switch2

D．Switch1→Switch0→Switch2

**【问题 4】（3 分）**

为了部门 A 中用户能够访问服务器 Server1，请在 R0 上配置一条特定主机路由。

R0（config）#ip route 202.114.10.253 ___（11）___ ___（12）___

**试题一分析**

本题涉及 IP 地址配置、VLAN 以及交换机路由器配置基本命令。

从网络拓扑图可以看出，R0 所在路由器 S0 端口掩码应为 255.255.255.0，同时，由于 S0 端口线路工作为帧中继，因此 S0 端口工作模式应配置为帧中继模式。

由于 Switch0、Switch1、Switch2 和 Switch3 均为二层交换机。根据拓扑图可以看出，在路由器 R2 的端口 e0/0 需要通过配置独臂路由实现 VLAN 间路由。根据 VLAN 的 IP 地址分配，路由器 e0/0 下的端口 e0/0.1 负责线路 VLAN 100，e0/0.2 负责线路 VLAN 200，e0/0.3 负责线路 VLAN 300。同时在 Switch0 的 f0/24 端口需要配置工作模式为 Trunk，允许通过不同 VLAN 的数据，VLAN 的封装协议为 802.1q。

主机 A 与 Switch1 之间线路为接入链路，因此需要将端口设置为接入链路模式，相应命令为 switchport mode access，同时主机 A 所处 VLAN 为 100，因此使用 switch access vlan 100 设定端口 VLAN 号为 100。

主机 A 与主机 D 属于不同 VLAN，同时由于不同 VLAN 间路由通过独臂路由实现，因此主机 A 的数据会通过路由器 R2 进行转发。

部门 A 中用户配置特定主机路由时，子网掩码需配置为 255.255.255.255，同时下一条目的地址应指向路由器 R1 的 S0/0 端口，相应 IP 地址为 202.114.13.2。

**参考答案**

**【问题 1】**

（1）225.255.255.0

（2）frame-relay

**【问题 2】**

（3）100

（4）200

（5）300

（6）trunk

（7）dot1q

**【问题3】**

（8）switchport mode access

（9）switch access vlan 100

（10）B

**【问题4】**

（11）255.255.255.255

（12）202.114.13.2

**试题二（共15分）**

阅读以下说明，回答问题1至问题6，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司总部服务器1的操作系统为Windows Server 2003，需安装虚拟专用网（VPN）服务，通过Internet与子公司实现安全通信，其网络拓扑结构和相关参数如图2-1所示。

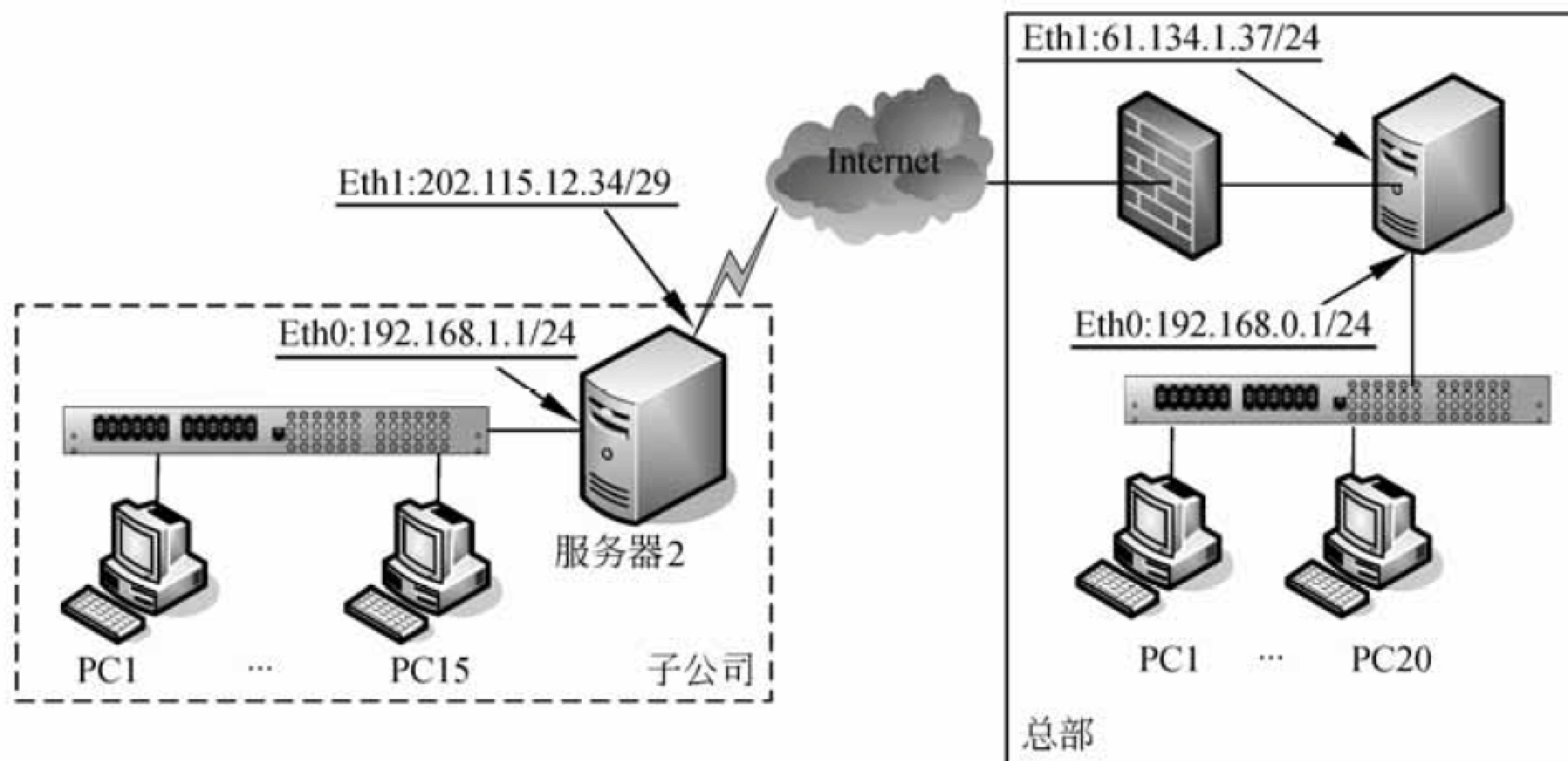



图2-1

**【问题1】（2分）**

在Windows Server 2003的“路由和远程访问”中提供两种隧道协议来实现VPN服务：（1）和L2TP，L2TP协议将数据封装在___（2）___协议帧中进行传输。

**【问题2】（1分）**

在服务器1中，利用Windows Server 2003的管理工具打开“路由和远程访问”，在所列出的本地服务器上选择“配置并启用路由和远程访问”，然后选择配置“远程访问（拨号或VPN）”服务，在图2-2所示的界面中，“网络接口”应选择___（3）___。

（3）备选答案：

A. 连接1　　　　B. 路由和远程访问

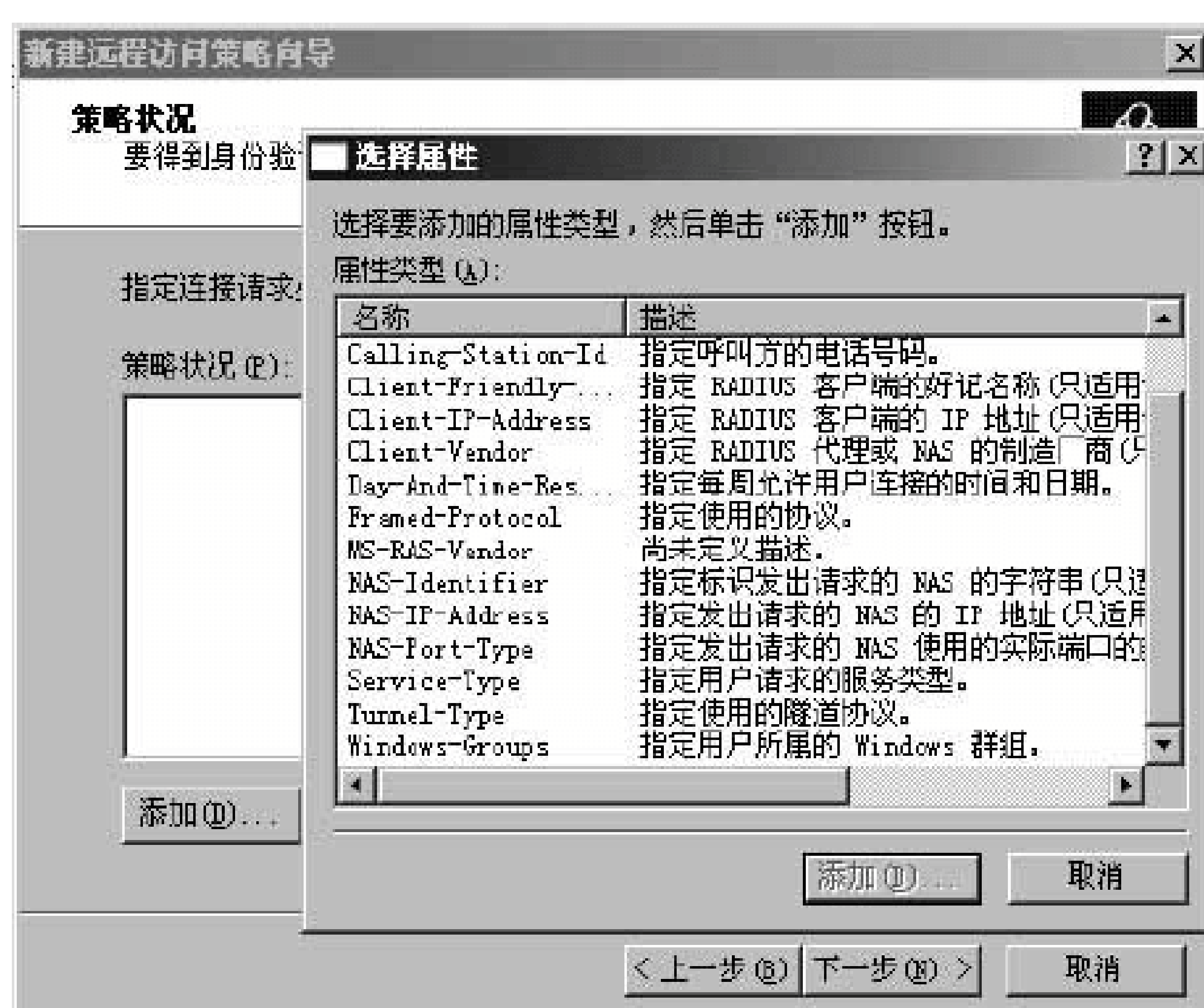



图 2-2

**【问题 3】（4 分）**

为了加强远程访问管理，新建一条名为“SubInc”的访问控制策略，允许来自子公司服务器 2 的 VPN 访问。在图 2-3 所示的配置界面中，应将“属性类型（A）”的名称为__（4）__的值设置为“Layer Two Tunneling Protocol”，名称为__（5）__的值设置为“Virtual（VPN）”。

编辑 SubInc 策略的配置文件，添加“入站 IP 筛选器”，在如图 2-4 所示的配置界面中，IP 地址应填为__（6）__，子网掩码应填为__（7）__。



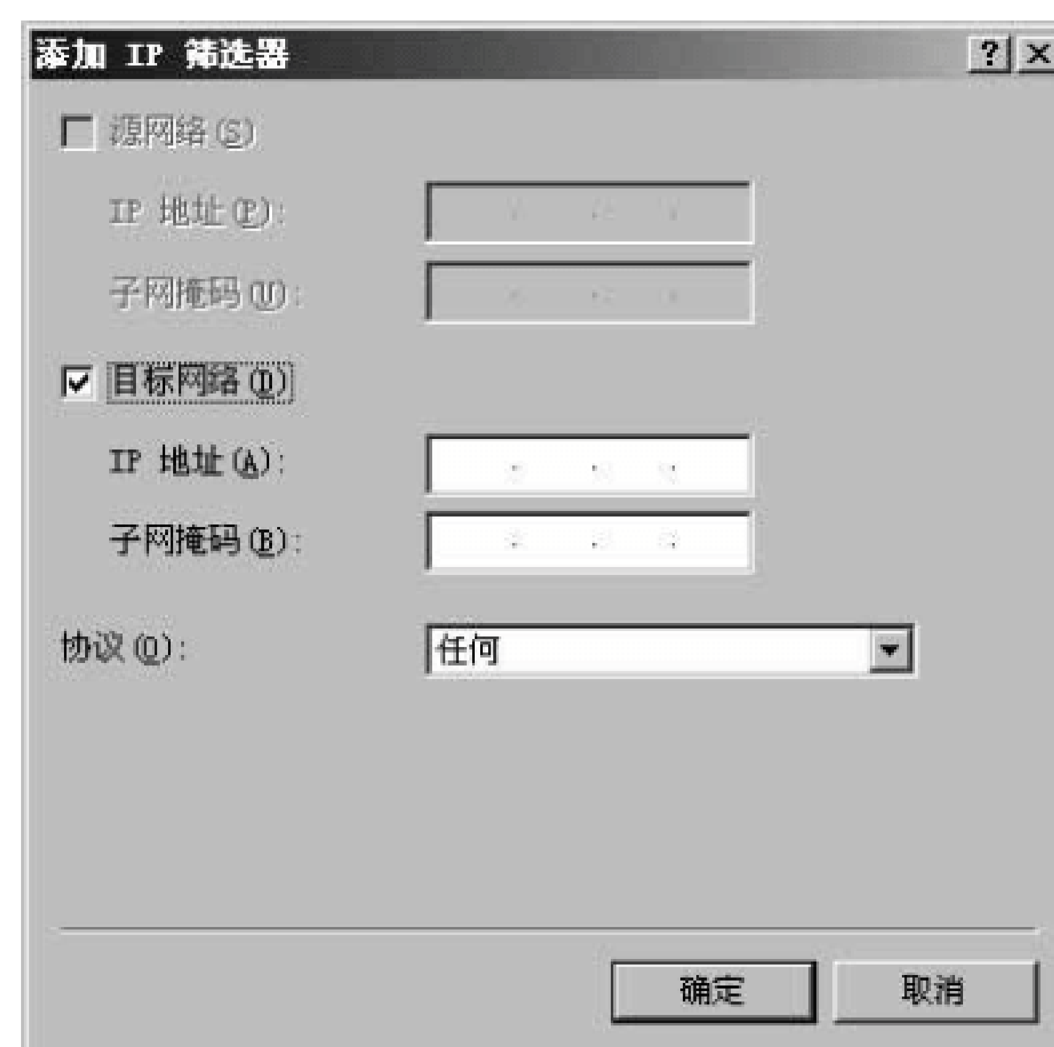




图 2-3　　　　　　　　　　图 2-4

**【问题 4】（4 分）**

子公司 PC1 安装 Windows XP 操作系统，打开“网络和 Internet 连接”。若要建立与公司总部服务器的 VPN 连接，在如图 2-5 所示的窗口中应该选择__（8）__，在图 2-6 所示的配置界面中填写__（9）__。

（8）备选答案：

A. 设置或更改您的 Internet 连接

B. 创建一个到您的工作位置的网络连接

C. 设置或更改您的家庭或小型办公网络

D. 为家庭或小型办公室设置无线网络

E. 更改 Windows 防火墙设置




图 2-5

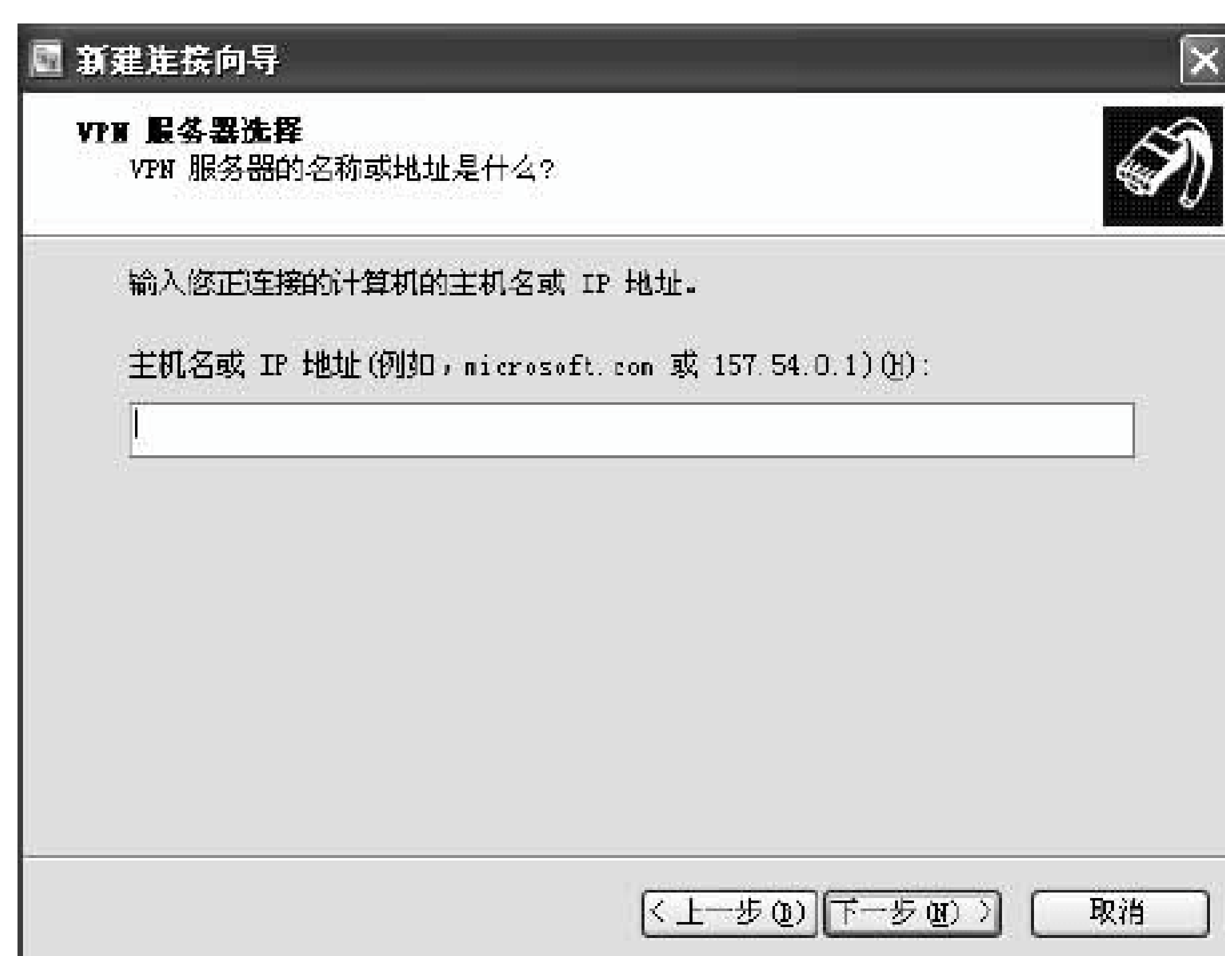



图 2-6

**【问题 5】（2 分）**

用户建立的 VPN 连接 xd2 的属性如图 2-7 所示，启动该 VPN 连接时是否需要输入用户名和密码？为什么？

**【问题 6】（2 分）**

图 2-8 所示的配置窗口中所列协议“不加密的密码（PAP）”和“质询握手身份验证协议（CHAP）”有何区别？




图 2-7




图 2-8

## 试题二分析

本题考查的是 VPN 及其配置问题。

**【问题 1】**

本问题考查的是“路由和远程访问”提供的两种用于创建路由器到路由器的 VPN 连接的隧道协议：点对点隧道协议（PPTP）和第二层隧道协议（L2TP）。PPTP 是一种

VPN 隧道协议，是点对点协议（PPP）的扩展，并利用 PPP 的身份验证、压缩和加密机制。L2TP 是一个工业标准 Internet 隧道协议，它先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。与 PPTP 一样，L2TP 也利用 PPP 的身份验证和压缩机制。但与 PPTP 不同的是，L2TP 不采用"Microsoft 点对点加密（MPPE）"来加密 PPP 帧。L2TP 依赖于加密服务的 Internet 协议安全性（IPSec）。

【问题 2】

本问题考查的是远程访问 VPN 服务的部署。

在 VPN 连接页，应选择连接到 Internet 的网络接口，因此应选择对应的接口连接 2。

【问题 3】

本问题考查的是远程访问策略的配置。

要配置远程访问策略以控制 VPN 连接的身份验证和加密选项，要使用以下设置创建远程访问策略：将 NAS-Port-Type 条件设置为"Virtual（VPN）"，并将 Tunnel-Type 条件设置为"Layer Two Tunneling Protocol"。在配置数据包筛选器时，要键入外部接口的 IP 地址。在"子网掩码"框中，键入 255.255. 255.255。

【问题 4】

本问题考查的是 VPN 客户端的配置。

客户端上应新建一个"到您的工作位置的网络连接"，在 VPN 服务器选择时，要键入 VPN 服务器计算机的 IP 地址或主机名。

【问题 5】

本问题考查的是 VPN 身份验证。

该 VPN 连接时是不需要输入用户名和密码的，因为选中了"自动使用我的 Windows 登录名和密码"，此时用本机 Windows 登录的用户名和密码进行 VPN 连接。

【问题 6】

本问题考查的是 PPP 协议定义的两种类型的认证。

握手认证协议（CHAP）使用一种算法（MD-5）来计算只有认证系统和远程设备知道的值。它总是对用户 ID 和密码进行加密，所以该协议比 PAP 更安全。此协议对回放和试错法访问企图有效。可以在连接期间执行多次 CHAP 认证。认证系统向正在尝试连接到网络的远程设备发送一个握手信号。远程设备通过由两个设备使用的公共算法（MD-5）所算出的值进行响应。认证系统对照自己的计算结果检查该响应。当这些值匹配时，认证被认可；否则，结束连接。

不加密的密码（PAP）使用双向握手为同级系统提供鉴别其身份的简单方法，也就是普通的口令认证，要求将密钥信息在通信信道中明文传输。在建立链接时进行握手。在建立链接之后，远程设备将一个用户 ID/密码对发送到认证系统。根据用户 ID/密码对的正确与否，认证系统继续连接或结束连接。

**参考答案**

【问题 1】

（1）PPTP（点对点隧道协议）

（2）PPP（点对点协议）

**【问题 2】**

（3）B

**【问题 3】**

（4）Tunnel-Type

（5）NAS-Port-Type

（6）202.115.12.34

（7）255.255.255.255

**【问题 4】**

（8）B

（9）61.134.1.37

**【问题 5】**

不需要。因为选中“自动使用我的 Windows 登录名和密码”，此时用本机 Windows 登录的用户名和密码进行 VPN 连接。

**【问题 6】**

PAP 使用明文身份验证。

CHAP 通过使用 MD5 和质询-响应机制提供一种加密身份验证。

**试题三（共 15 分）**

阅读以下关于 Linux 文件系统和 Samba 服务的说明，回答问题 1 至问题 3。

**【说明】**

Linux 系统采用了树型多级目录来管理文件，树型结构的最上层是根目录，其他的所有目录都是从根目录生成的。

通过 Samba 可以实现基于 Linux 操作系统的服务器和基于 Windows 操作系统的客户机之间的文件、目录及共享打印服务。

**【问题 1】（6 分）**

Linux 在安装时会创建一些默认的目录，如下表所示：

| / | |
|---|---|
| /bin | |
| /boot | 存放启动系统使用的文件 |
| /dev | |
| /etc | 用来存放系统管理所需要的配置文件和子目录 |
| /home | |
| /lib | 文件系统中程序所需要的共享库 |
| /lost+found | |
| /mnt | 临时安装（mount）文件系统的挂载点 |
| /opt | |
| /proc | |
| /root | |
| /sbin | |
| /usr | |
| /var | 包含系统运行时要改变的数据 |
| /tmp | |

依据上述表格，在空（1）～（6）中填写恰当的内容（其中空（1）在候选答案中选择）。

① 对于多分区的 Linux 系统，文件目录树的数目是__（1）__。

② Linux 系统的根目录是__（2）__，默认的用户主目录在__（3）__目录下，系统的设备文件（如打印驱动）存放在__（4）__目录中，__（5）__目录中的内容关机后不能被保存。

③ 如果在工作期间突然停电，或者没有正常关机，在重新启动机器时，系统将要复查文件系统，系统将找到的无法确定位置的文件放到目录__（6）__中。

（1）备选答案：

A．1　　B．分区的数目　　C．大于 1

**【问题 2】（4 分）**

默认情况下，系统将创建的普通文件的权限设置为-rw-r--r--，即文件所有者对文件__（7）__，同组用户对文件__（8）__，其他用户对文件__（9）__。文件的所有者或者超级用户，采用__（10）__命令可以改变文件的访问权限。

**【问题 3】（5 分）**

Linux 系统中 Samba 的主要配置文件是/etc/samba/smb.conf。请根据以下的 smb.conf 配置文件，在空（11）～（15）中填写恰当的内容。

Linux 服务器启动 Samba 服务后，在客户机的“网络邻居”中显示提供共享服务的 Linux 主机名为__（11）__，其共享的服务有__（12）__，能够访问 Samba 共享服务的客户机的地址范围__（13）__；能够通过 Samba 服务读写/home/samba 中内容的用户是__（14）__；该 Samba 服务器的安全级别是__（15）__。

```
[global]
workgroup = MYGROUP
netbios name=smb-server
server string = Samba Server
;hosts allow = 192.168.1. 192.168.2. 127.
load printers = yes
security = user
[printers]
comment = My Printer
browseable = yes
path = /usr/spool/samba
guest ok = yes
writable = no
printable = yes
[public]
comment = Public Test
```

```
browseable = no
path = /home/samba
public = yes
writable = yes
printable = no
write list = @test
[user1dir]
comment = User1's Service
browseable = no
path = /usr/usr1
valid users = user1
public = no
writable = yes
printable = no
```

**试题三分析**

Linux 系统中每个分区都是一个文件系统，Linux 将这些分属不同分区、单独的文件系统按一定的方式形成一个系统的总目录层次结构，即一个目录树。

Linux 使用树型目录结构管理文件和目录。树型结构由一个根目录（root）和根目录下的子目录构成，每一个目录内可以包含下一级目录、文件、指向其他文件系统的符号链接、表示设备的设备名（如/dev/had）。

Linux 系统主要的目录项包括：

| / | 根目录，其他文件都在根目录的子目录中 |
|---|---|
| /bin | 存放用户可执行的命令，如 ls 等等 |
| /boot | 存放启动系统使用的文件 |
| /dev | 外部设备文件所在目录 |
| /etc | 用来存放系统管理所需要的配置文件和子目录 |
| /home | 用户的主目录 |
| /lib | 文件系统中程序所需要的共享库 |
| /lost+found | 用于存放系统收集到的无法确定位置的文件 |
| /mnt | 临时安装（mount）文件系统的挂载点 |
| /opt | 可选文件和程序的存储目录 |
| /proc | 由系统内核在内存中产生的目录，并不存在于硬盘上 |
| /root | 系统管理员（超级用户）的主目录 |
| /sbin | 存放系统管理员使用的系统程序 |
| /usr | 所有安装的程序都在此目录中 |
| /var | 包含系统运行时要改变的数据 |
| /tmp | 存放临时文件 |
| /var | 包含系统一般运行时要改变的数据（参数） |

Linux 文件的访问权限有 4 种：读（r）、写（w）、执行（x）和无权（-）。对于目录来说，执行权限允许用户进入该目录。对每个文件可以指定三种存取控制权限：文件所有者对文件所拥有的存取权限，文件所有者所在组对文件所拥有的存取权限，其他任意用户对文件所拥有的存取权限。根用户（root）具有对一切目录和文件的控制权限并可以指定对任何一个文件和目录的存取权限，一般用户只能对自己建立的文件和目录制定存取权限。默认情况下，系统将创建的普通文件的权限设置为-rw-r-r--，即文件所有者对该文件可读可写（rw），而同组用户和其他用户都只可读；同样，在默认配置中，将每一个用户所有者目录的权限都设置为 drwx------，即只有文件所有者对该目录可读、写和可查询，也意味着用户不能读其他用户目录中的内容。

chmod（change mode 的简写）命令用于改变文件或目录的访问权限。只有文件所有者或超级用户 root 才有权用 chmod 改变文件或目录的访问权限。

Samba 是一个基于 SMB（Server Message Block）协议的功能强大的软件工具，可以实现基于 Linux 操作系统的文件/目录及打印机共享服务。SMB 是一种客户端/服务器协议，SMB 客户端使用 TCP/IP、NetBEUI 或 IPX/SPX 与服务器连接。当工作在 TCP/IP 网络上时，通过 NetBIOS nameserver 使网络中 Linux 系统用户的机器可以在 Windows 系统的网络邻居上被看到。

Samba 安装完成后，通过配置/etc/samba/smb.conf 文件，才能使其有效工作，该配置文件的部分重要参数说明如下。

- [global]：配置文件中关于全局参数的设置部分。
- workgroup= MYGROUP：这是设置服务器所要加入的工作组的名称。
- netbios name= smb-server：设置出现在“网上邻居”中的主机名。
- server string = Samba Server：设置服务器主机的说明信息。
- ;hosts allow= 192.168.1. 192.168.2. 127. ：用于限制可以访问 samba 服务器的客户端的 IP 地址范围。默认情况下，这行配置被注释掉了（左边是;号的是注释行），表示允许所有 IP 地址的主机都可以访问这台 samba 服务器。
- security=user：设置 samba 服务器的安全等级。Samba 服务器一共有 4 种安全等级，分别是 share（共享安全级）、user（用户安全级）、server（服务器安全级）和 domain（域安全级）。
- [public]等：共享资源的名称。
- comment=：针对共享资源所做的说明、注释部分。
- browseable=：设置用户是否可以看到此共享资源，默认值是 yes。
- writable=：共享的资源是否可以写入。
- valid users=：指定允许使用服务的用户列表。
- write list=：设置读写访问用户列表，参数@后的名称表示用户组。

## 参考答案

**【问题 1】**

（1）A

（2）/

（3）/home

（4）/dev

（5）/proc

（6）/lost+found

**【问题 2】**

（7）可读、可写

（8）仅可读

（9）仅可读

（10）chmod

**【问题 3】**

（11）smb-server

（12）printers 或 My Printer

（13）无限制（因为 hosts allow 被分号注释掉了）

（14）Linux 系统的 test 组中用户（仅回答 test 用户不给分）

（15）用户安全级

## 试题四（共 15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司总部和分支机构的网络配置如图 4-1 所示。在路由器 R1 和 R2 上配置 IPSec 安全策略，实现分支机构和总部的安全通信。

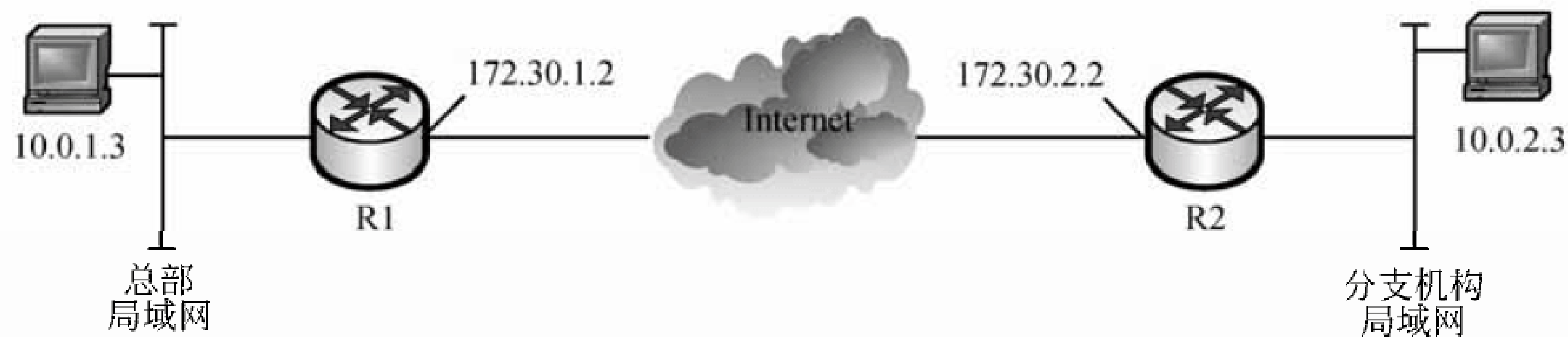



图 4-1

**【问题 1】**（4 分）

图 4-2 中（a）、（b）、（c）、（d）为不同类型 IPSec 数据包的示意图，其中__（1）__和__（2）__工作在隧道模式；__（3）__和__（4）__支持报文加密。




图 4-2

**【问题 2】（4 分）**

下面的命令在路由器 R1 中建立 IKE 策略，请补充完成命令或说明命令的含义。

```
R1 (config) # crypto isakmp policy 110       进入 ISAKMP 配置模式
R1 (config-isakmp) # encryption des           ____(5)____
R1 (config-isakmp) # ____(6)____              采用 MD5 散列算法
R1 (config-isakmp) # authentication pre-share     ____(7)____
R1 (config-isakmp) # group 1
R1 (config-isakmp) # lifetime ____(8)____     安全关联生存期为 1 天
```

**【问题 3】（4 分）**

R2 与 R1 之间采用预共享密钥“12345678”建立 IPSec 安全关联，请完成下面配置命令。

```
R1 (config) # crypt isakmp key 12345678 address ____(9)____
R2 (config) # crypt isakmp key 12345678 address ____(10)____
```

**【问题 4】（3 分）**

完成以下 ACL 配置，实现总部主机 10.0.1.3 和分支机构主机 10.0.2.3 的通信。

```
R1 (config) # access-list 110 permit ip host ____(11)____ host ____(12)____
R2 (config) # access-list 110 permit ip host ____(13)____ host 10.0.1.3
```

**试题四分析**

本题考查考生在路由器上配置 IPSec 安全策略的实际操作能力。考点涉及到 IPSec 的基本概念和相关的配置命令。

**【问题 1】**

本问题考查 IPSec 的基本概念。

IPSec 支持认证头（AH）协议和封装安全有效载荷（ESP）协议，其中认证头协议仅支持认证，不支持加密；封装安全有效载荷协议既支持认证又支持加密。IPSec 有两种工作模式，分别是传输模式和隧道模式，工作在传输模式时，AH 或 ESP 被插入到 IP 头和有效载荷之间；工作在隧道模式时，在 AH 或 ESP 前面会生成一个新的 IP 头。从图 4-2 中可以看出，(a)、(c) 支持的是 AH 协议，(b)、(d) 支持的是 ESP 协议，(a)、(b) 工作在传输模式，(c)、(d) 工作在隧道模式。所以 (1)、(2) 答案为 c 和 d；(3)、(4)

答案为 b 和 d。

【问题 2】

本问题考查 IKE 策略的建立步骤和命令。

配置 IKE 的策略配置主要包含以下方面：

- 加密算法 encryption 默认 DES。
- 散列算法 hash 默认 SHA。
- 密钥交换 group 默认 1。
- 验证方法 authentication 默认 rsa-si，如果使用 pre-share 则在路由器中配置 key。
- IKE SA 生命周期 lefttime 默认 86 400s（1 天）。

空（5）对应命令的解释为“加密算法为 DES”；空（6）提示要求采用 MD5 散列算法，对应命令为“hash md5”；空（7）对应命令为采用预共享密钥认证；空（8）要求安全关联生存期为 1 天，对应命令为 lifetime 86400（单位为秒：1 天=24×3600 秒）。

【问题 3】

本问题考查预共享密钥的设置。

在路由器 R1 与 R2 之间需要分别配置对方的预共享密钥，路由器 R1 与 R2 的对方分别是 R2 和 R1，所以（9）、（10）分别是 R2 和 R1 的 IP 地址 172.30.2.2 和 172.30.1.2。

【问题 4】

本问题考查 ACL 配置。

为了实现 10.0.1.3 和 10.0.2.3 的通信，需要分别在路由器 R1 和 R2 上作相应的 ACL 配置，R1 的配置为允许 10.0.1.3 到 10.0.2.3 的 IP 包，R2 的配置为允许 10.0.2.3 到 10.0.1.3 的 IP 包。根据扩展 ACL 配置命令语法：

```
Router (config) #access-list access-list-number { permit | deny } protocol
[ source source-wildcard destination destination-wildcard ] [operator port]
[established] [log]
```

空（11）为源主机 IP 地址 10.0.1.3，空（12）为目标主机 IP 地址 10.0.2.3，空（13）为源主机 IP 地址 10.0.2.3。

**参考答案**

【问题 1】

（1）、（2） c、d （顺序可交换）

（3）、（4） b、d （顺序可交换）

【问题 2】

（5）加密算法为 DES

（6）hash md5

（7）认证采用预共享密钥

（8）86400

【问题 3】

（9）172.30.2.2

（10）172.30.1.2

【问题 4】

（11）10.0.1.3

（12）10.0.2.3

（13）10.0.2.3

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位采用双出口网络，其网络拓扑结构如图 5-1 所示。

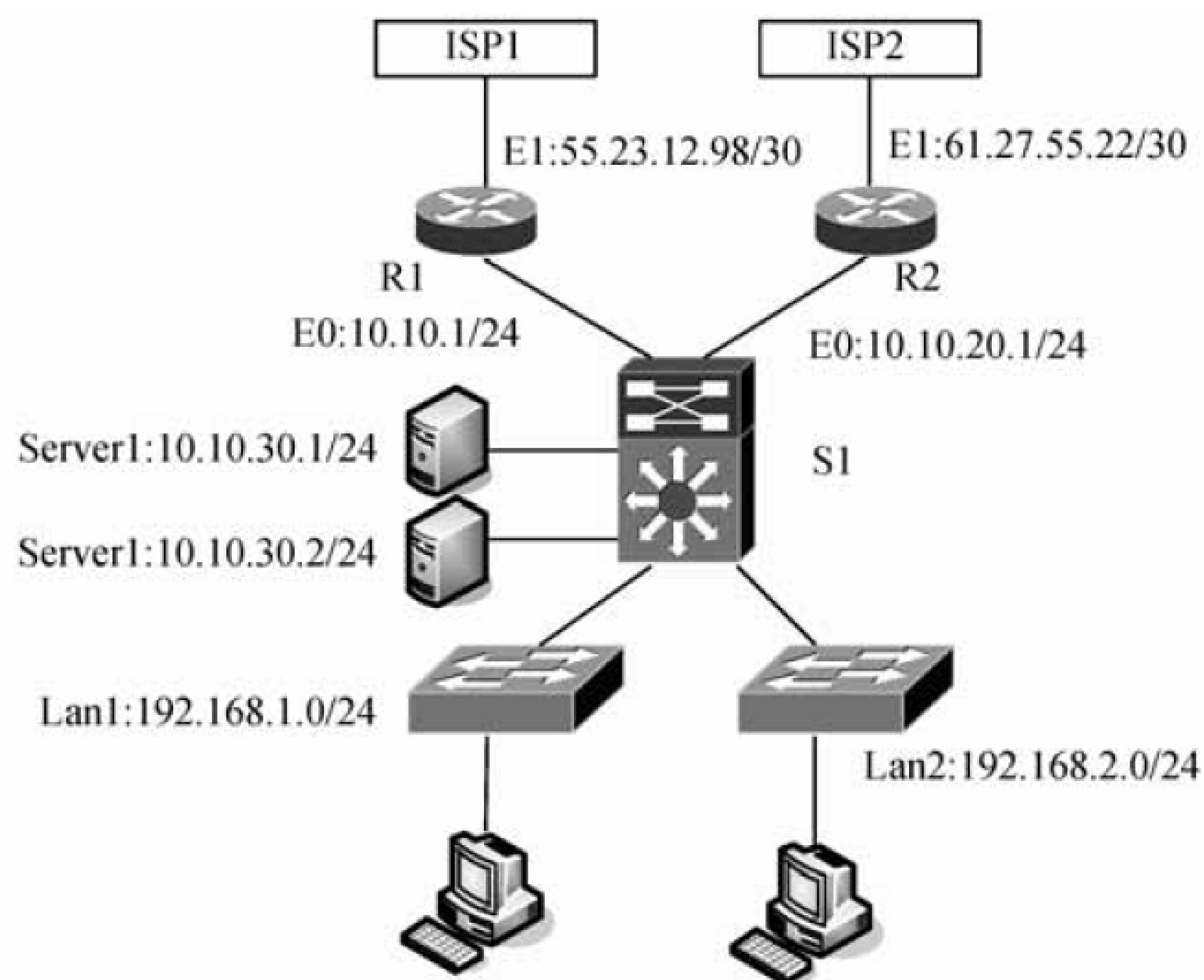



图 5-1

该单位根据实际需要，配置网络出口实现如下功能：

（1）单位网内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经 ISP2；

（2）单位网内用户访问其他 IP 地址时，出口经 ISP1；

（3）服务器通过 ISP2 线路为外部提供服务。

**【问题 1】（5 分）**

在该单位的三层交换机 S1 上，根据上述要求完成静态路由配置。

```
ip route ___(1)___                                  （设置默认路由）
ip route 158.124.0.0     ___(2)___ ___(3)___        （设置静态路由）
ip route 158.153.208.0   ___(4)___ ___(5)___        （设置静态路由）
```

**【问题 2】（6 分）**

1．根据上述要求，在三层交换机 S1 上配置了两组 ACL，请根据题目要求完成以下配置。

```
access -list 10 permit ip host 10.10.30.1 any
access -list 10 permit ip host ___(6)___ any
access -list 12 permit ip any 158.124.0.0 ___(7)___
```

```
access -list 12 permit ip any 158.153.208.0 ___(8)___
access -list 12 deny  ip any any
```

2．完成以下策略路由的配置。

```
route-map test permit 10
___(9)___ ip address 10
___(10)___ ip next-hop ___(11)___
```

**【问题 3】（4 分）**

以下是路由器 R1 的部分配置。请完成配置命令。

```
R1（config）#interface fastethernet0/0
R1（config-if）#ip address ___(12)___ ___(13)___
R1（config-if）ip nat inside
...
R1（config）#interface fastethernet0/1
R1（config-if）#ip address ___(14)___ ___(15)___
R1（config-if）ip nat outside
...
```

**试题五分析**

本题考查的是局域网双出口的配置及 ACL 设置问题。

**【问题 1】**

本问题考查的是路由器静态路由的设置方法。

根据题目要求，该网络内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经 ISP2，由图 5-1 可知，其端口地址为 10.10.20.1/24，网内用户访问其他 IP 地址时，出口经 ISP1，由图 5-1 可知，其端口地址为 10.10.10.1/24。所以，在该单位的三层交换机 S1 上，静态路由配置如下：

```
ip route 0.0.0.0     0.0.0.0 10.10.10.1
ip route 158.124.0.0    255.254.0.0 10.10.20.1
ip route 158.153.208.0  255.255.240.0 10.10.20.1
```

**【问题 2】**

本问题考查的是 ACL 设置及策略路由配置问题。

根据题目要求可知，服务器通过 ISP2 线路为外部提供服务，另外单位网内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经 ISP2。

access -list 10 结合策略路由，保证服务器通过 ISP2 线路为外部提供服务，所以 access -list 10 内容如下：

```
access -list 10 permit ip host 10.10.30.1 any
access -list 10 permit ip host 10.10.30.2  any
```

对应的策略路由为：

```
route-map test permit 10
```

```
match ip address 10
set ip next-hop 10.10.20.1
```

access -list 12 配置网内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经 ISP2，所以配置如下：

```
access -list 12 permit ip any 158.124.0.0   0.1.255.255
access -list 12 permit ip any 158.153.208.0  0.0.15.255
access -list 12 deny  ip any any
```

**【问题 3】**

本问题考查的是路由器的配置问题。

由图 5-1 可知，路由器 R1 的内网 IP 为 10. 10.10.1/24，外网 IP 地址为 55.23.12.98/30，所以其地址配置如下：

```
R1 (config) #interface fastethernet0/0
R1 (config-if) #ip address  10.10.10.1 255.255.255.0
R1 (config-if) ip nat inside
...
R1 (config) #interface fastethernet0/1
R1 (config-if) #ip address  55.23.12.98  255.255.255.252
R1 (config-if) ip nat outside
```

**参考答案**

**【问题 1】**

（1）0.0.0.0 0.0.0.0 10.10.10.1

（2）255.254.0.0

（3）10.10.20.1

（4）255.255.240.0

（5）10.10.20.1

**【问题 2】**

（6）10.10.30.2

（7）0.1.255.255

（8）0.0.15.255

（9）match

（10）set

（11）10.10.20.1

**【问题 3】**

（12）10.10.10.1

（13）255.255.255.0

（14）55.23.12.98

（15）255.255.255.252

# 第 3 章　2009 下半年网络工程师上午试题分析与解答

**试题（1）**

以下关于 CPU 的叙述中，错误的是__（1）__。

（1）A. CPU 产生每条指令的操作信号并将操作信号送往相应的部件进行控制

B. 程序计数器 PC 除了存放指令地址，也可以临时存储算术/逻辑运算结果

C. CPU 中的控制器决定计算机运行过程的自动化

D. 指令译码器是 CPU 控制器中的部件

**试题（1）分析**

本题考查计算机硬件组成基础知识。

CPU 是计算机的控制中心，主要由运算器、控制器、寄存器组和内部总线等部件组成。控制器由程序计数器、指令寄存器、指令译码器、时序产生器和操作控制器组成，它是发布命令的"决策机构"，即完成协调和指挥整个计算机系统的操作。它的主要功能有：从内存中取出一条指令，并指出下一条指令在内存中的位置；对指令进行译码或测试，并产生相应的操作控制信号，以便启动规定的动作；指挥并控制 CPU、内存和输入输出设备之间数据的流动。

程序计数器（PC）是专用寄存器，具有寄存信息和计数两种功能，又称为指令计数器，在程序开始执行前，将程序的起始地址送入 PC，该地址在程序加载到内存时确定，因此 PC 的初始内容即是程序第一条指令的地址。执行指令时，CPU 将自动修改 PC 的内容，以便使其保持的总是将要执行的下一条指令的地址。由于大多数指令都是按顺序执行的，因此修改的过程通常只是简单地对 PC 加 1。当遇到转移指令时，后继指令的地址根据当前指令的地址加上一个向前或向后转移的位移量得到，或者根据转移指令给出的直接转移的地址得到。

**参考答案**

（1）B

**试题（2）**

以下关于 CISC（Complex Instruction Set Computer，复杂指令集计算机）和 RISC（Reduced Instruction Set Computer，精简指令集计算机）的叙述中，错误的是__（2）__。

（2）A. 在 CISC 中，其复杂指令都采用硬布线逻辑来执行

B. 采用 CISC 技术的 CPU，其芯片设计复杂度更高

C. 在 RISC 中，更适合采用硬布线逻辑执行指令

D. 采用 RISC 技术，指令系统中的指令种类和寻址方式更少

**试题（2）分析**

本题考查指令系统和计算机体系结构基础知识。

CISC（Complex Instruction Set Computer，复杂指令集计算机）的基本思想是：进一步增强原有指令的功能，用更为复杂的新指令取代原先由软件子程序完成的功能，实现软件功能的硬件化，导致机器的指令系统越来越庞大而复杂。CISC 计算机一般所含的指令数目至少 300 条以上，有的甚至超过 500 条。

RISC（Reduced Instruction Set Computer，精简指令集计算机）的基本思想是：通过减少指令总数和简化指令功能，降低硬件设计的复杂度，使指令能单周期执行，并通过优化编译提高指令的执行速度，采用硬布线控制逻辑优化编译程序。在 20 世纪 70 年代末开始兴起，导致机器的指令系统进一步精炼而简单。

**参考答案**

（2）A

**试题（3）**

以下关于校验码的叙述中，正确的是__（3）__。

（3）A. 海明码利用多组数位的奇偶性来检错和纠错

B. 海明码的码距必须大于等于 1

C. 循环冗余校验码具有很强的检错和纠错能力

D. 循环冗余校验码的码距必定为 1

**试题（3）分析**

本题考查校验码的基础知识。

一个编码系统中任意两个合法编码（码字）之间不同的二进数位数称为这两个码字的码距，而整个编码系统中任意两个码字的最小距离就是该编码系统的码距。为了使一个系统能检查和纠正一个差错，码间最小距离必须至少是 3。

海明码是一种可以纠正一位差错的编码，是利用奇偶性来检错和纠错的校验方法。海明码的基本意思是给传输的数据增加 $r$ 个校验位，从而增加两个合法消息（合法码字）的不同位的个数（海明距离）。假设要传输的信息有 $m$ 位，则经海明编码的码字就有 $n=m+r$ 位。

循环冗余校验码（CRC）编码方法是在 $k$ 位信息码后再拼接 $r$ 位的校验码，形成长度为 $n$ 位的编码，其特点是检错能力极强且开销小，易于用编码器及检测电路实现。

在数据通信与网络中，通常 $k$ 相当大，由一千甚至数千数据位构成一帧，而后采用 CRC 码产生 $r$ 位的校验位。它只能检测出错误，而不能纠正错误。一般取 $r$=16，标准的 16 位生成多项式有 CRC–16= $x^{16}+x^{15}+x^{2}+1$ 和 CRC–CCITT= $x^{16}+x^{12}+x^{5}+1$。一般情况下，$r$ 位生成多项式产生的 CRC 码可检测出所有的双错、奇数位错和突发长度小于等于 $r$ 的突发错。用于纠错目的的循环码的译码算法比较复杂。

**参考答案**

（3）A

**试题（4）**

以下关于 Cache 的叙述中，正确的是__（4）__。

（4）A. 在容量确定的情况下，替换算法的时间复杂度是影响 Cache 命中率的关键因素
B. Cache 的设计思想是在合理成本下提高命中率
C. Cache 的设计目标是容量尽可能与主存容量相等
D. CPU 中的 Cache 容量应大于 CPU 之外的 Cache 容量

**试题（4）分析**

本题考查高速缓存基础知识。

Cache 是一个高速小容量的临时存储器，可以用高速的静态存储器（SRAM）芯片实现，可以集成到 CPU 芯片内部，或者设置在 CPU 与内存之间，用于存储 CPU 最经常访问的指令或者操作数据。Cache 的出现是基于两种因素：首先是由于 CPU 的速度和性能提高很快而主存速度较低且价格高，其次是程序执行的局部性特点。因此，才将速度比较快而容量有限的 SRAM 构成 Cache，目的在于尽可能发挥 CPU 的高速度。很显然，要尽可能发挥 CPU 的高速度，就必须用硬件实现其全部功能。

**参考答案**

（4）B

**试题（5）**

面向对象开发方法的基本思想是尽可能按照人类认识客观世界的方法来分析和解决问题，__（5）__方法不属于面向对象方法。

（5）A. Booch　B. Coad　C. OMT　D. Jackson

**试题（5）分析**

本题考查面向对象开发方法。

面向对象开发方法有 Booch 方法、Coad 方法和 OMT 方法。Jackson 方法是一种面向数据结构的开发方法。

**参考答案**

（5）D

**试题（6）**

确定构建软件系统所需要的人数时，无需考虑__（6）__。

（6）A. 系统的市场前景　B. 系统的规模
C. 系统的技术复杂性　D. 项目计划

**试题（6）分析**

本题考查项目管理内容。

在对软件开发资源进行规划时，为了确定构建软件系统所需的人数，需要考虑软件

系统的规模、系统的技术复杂性、项目计划和开发人员的技术背景等方面，而与系统是否有市场前景无关。

**参考答案**

（6）A

**试题（7）**

一个项目为了修正一个错误而进行了变更。但这个错误被修正后，却引起以前可以正确运行的代码出错。__（7）__最可能发现这一问题。

（7）A. 单元测试　　B. 接受测试
C. 回归测试　　D. 安装测试

**试题（7）分析**

本题考查软件测试知识。

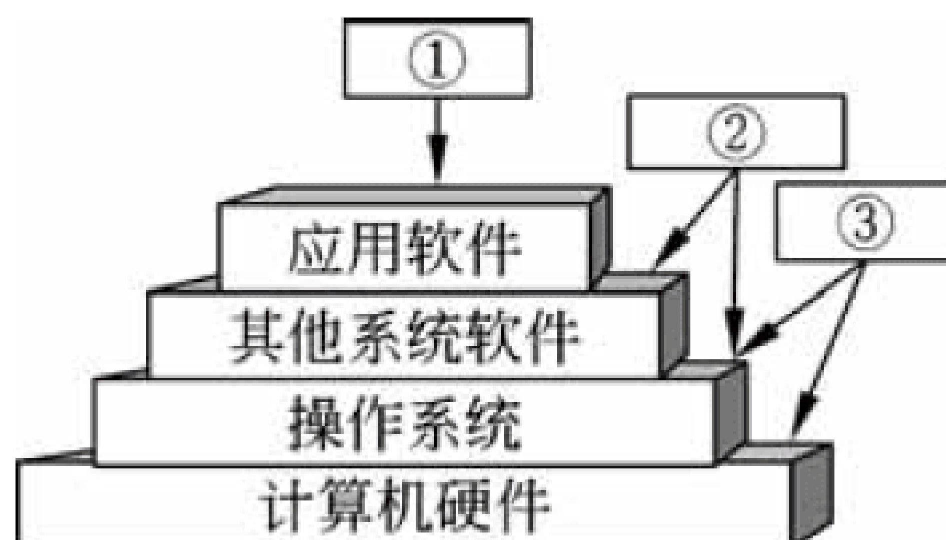
回归测试是在软件发生变更之后进行的测试，以发现在变更时可能引起的其他错误。

**参考答案**

（7）C

**试题（8）、（9）**

操作系统是裸机上的第一层软件，其他系统软件（如__（8）__等）和应用软件都是建立在操作系统基础上的。下图①②③分别表示__（9）__。




（8）A. 编译程序、财务软件和数据库管理系统软件
B. 汇编程序、编译程序和 Java 解释器
C. 编译程序、数据库管理系统软件和汽车防盗程序
D. 语言处理程序、办公管理软件和气象预报软件

（9）A. 应用软件开发者、最终用户和系统软件开发者
B. 应用软件开发者、系统软件开发者和最终用户
C. 最终用户、系统软件开发者和应用软件开发者
D. 最终用户、应用软件开发者和系统软件开发者

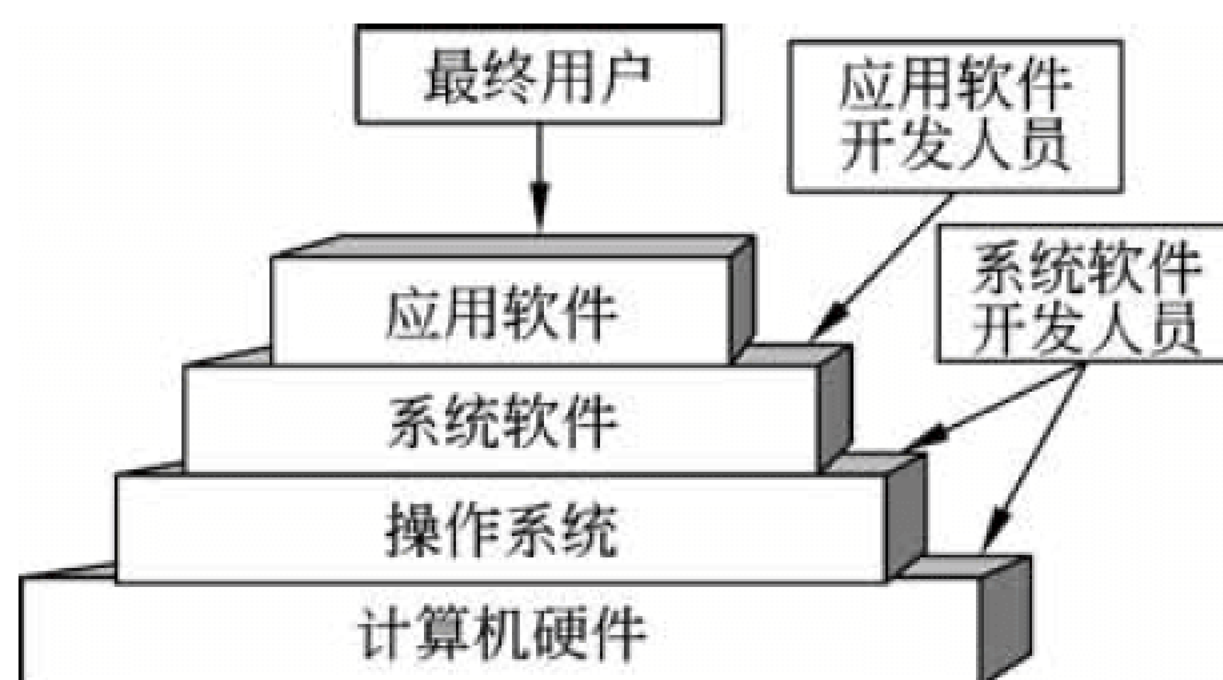
**试题（8）、（9）分析**

本题考查操作系统基本概念。

财务软件、汽车防盗程序、办公管理软件和气象预报软件都属于应用软件，而选项

A、C 和 D 中含有这些软件。选项 B 中汇编程序、编译程序和数据库管理系统软件都属于系统软件。

计算机系统由硬件和软件两部分组成。通常把未配置软件的计算机称为裸机，直接使用裸机不仅不方便，而且将严重降低工作效率和机器的利用率。操作系统（Operating System）的目的是为了填补人与机器之间的鸿沟，即建立用户与计算机之间的接口而为裸机配置的一种系统软件。由下图可以看出，操作系统是裸机上的第一层软件，是对硬件系统功能的首次扩充。它在计算机系统中占据重要而特殊的地位，所有其他软件，如编辑程序、汇编程序、编译程序和数据库管理系统等系统软件，以及大量的应用软件都是建立在操作系统基础上的，并得到它的支持和取得它的服务。从用户角度看，当计算机配置了操作系统后，用户不再直接使用计算机系统硬件，而是利用操作系统所提供的命令和服务去操纵计算机，操作系统已成为现代计算机系统中必不可少的最重要的系统软件，因此把操作系统看作是用户与计算机之间的接口。因此，操作系统紧贴系统硬件之上，所有其他软件之下（是其他软件的共同环境）。




操作系统在计算机系统中的地位示意图

**参考答案**

（8）B （9）D

**试题（10）**

软件权利人与被许可方签订一份软件使用许可合同。若在该合同约定的时间和地域范围内，软件权利人不得再许可任何第三人以此相同的方法使用该项软件，但软件权利人可以自己使用，则该项许可使用是__（10）__。

（10）A. 独家许可使用 B. 独占许可使用

C. 普通许可使用 D. 部分许可使用

**试题（10）分析**

软件许可使用一般有独占许可使用、独家许可使用和普通许可使用三种形式。独占许可使用，许可的是专有使用权，实施独占许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人自己不能使用该软件；独家许可使用，许可的是专有使用

权，实施独家许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人自己可以使用该软件；普通许可使用，许可的是非专有使用权，实施普通许可使用后，软件著作权人可以将软件使用权授予第三方，软件著作权人自己可以使用该软件。

**参考答案**

（10）B

**试题（11）、（12）**

E1 载波的基本帧由 32 个子信道组成，其中 30 个子信道用于传送话音数据，2 个子信道__（11）__用于传送控制信令，该基本帧的传送时间为__（12）__。

（11）A. CH0 和 CH2　B. CH1 和 CH15　C. CH15 和 CH16　D. CH0 和 CH16

（12）A. 100ms　B. 200μs　C. 125μs　D. 150μs

**试题（11）、（12）分析**

E1 载波的基本帧划分为 32 个子信道（E0），每个子信道含 8 位数据，子信道 CH0（或 TS0）用于组帧，使得接收方可以检测帧的开起点。另一个子信道 CH 16（或 TS16）用于承载控制呼叫的信令（例如 CAS 信令）。其余 30 个子信道用于承载 PCM 编码的话音数据。E1 帧每秒发送 8000 次，发送时间为 125μs，其数据速率为 8×32×8000=2.048Mb/s。

基于 E0 的准同步数字系列 PDH（Plesiochronous Digital Hierarchy）以 4 个低级信道组成更高一级的信道，如下图所示。实际使用的是 E1 和 E3 信道。

| Signal | Rate |
|---|---|
| E0 | 64 kb/s |
| E1 | 2.048 Mb/s |
| E2 | 8.448 Mb/s |
| E3 | 34.368 Mb/s |
| E4 | 139.264 Mb/s |

**参考答案**

（11）D　（12）C

**试题（13）、（14）**

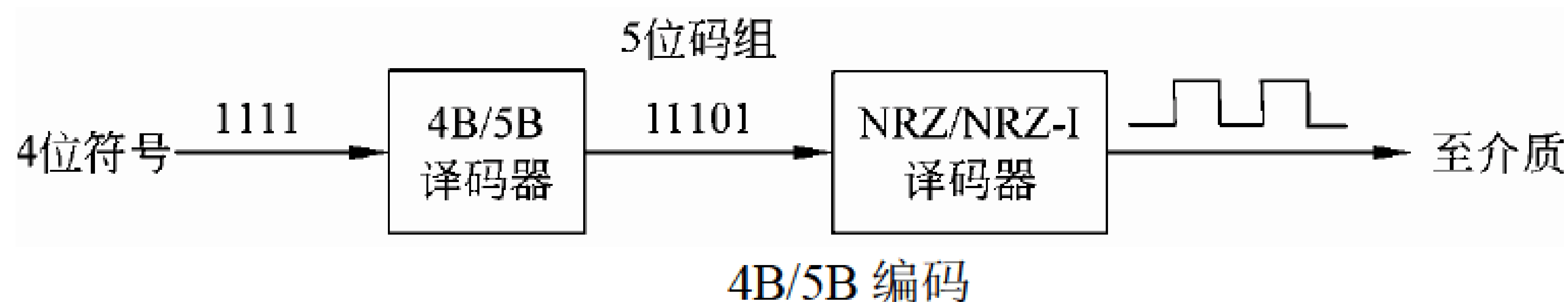
4B/5B 编码是一种两级编码方案，首先要把数据变成__（13）__编码，再把 4 位分为一组的代码变换成 5 单位的代码。这种编码的效率是__（14）__。

（13）A. NRZ-I　B. AMI　C. QAM　D. PCM

（14）A. 0.4　B. 0.5　C. 0.8　D. 1.0

**试题（13）、（14）分析**

采用 4B/5B 编码能够提高编码的效率，降低电路成本。这种编码方法的原理如下图所示。




4B/5B 编码

这实际上是一种两级编码方案。系统中使用不归零码（NRZ），在发送到传输介质时要变成见 1 就翻不归零码（NRZ-I）。NRZ-I 代码序列中 1 的个数越多，越能提供同步信息，如果遇到长串的“0”，则不能提供同步信息，所以在发送到介质上之前还需经过一次 4B/5B 编码。发送器扫描要发送的位序列，4 位分为一组，然后按照对应规则变换成 5 位二进制代码。

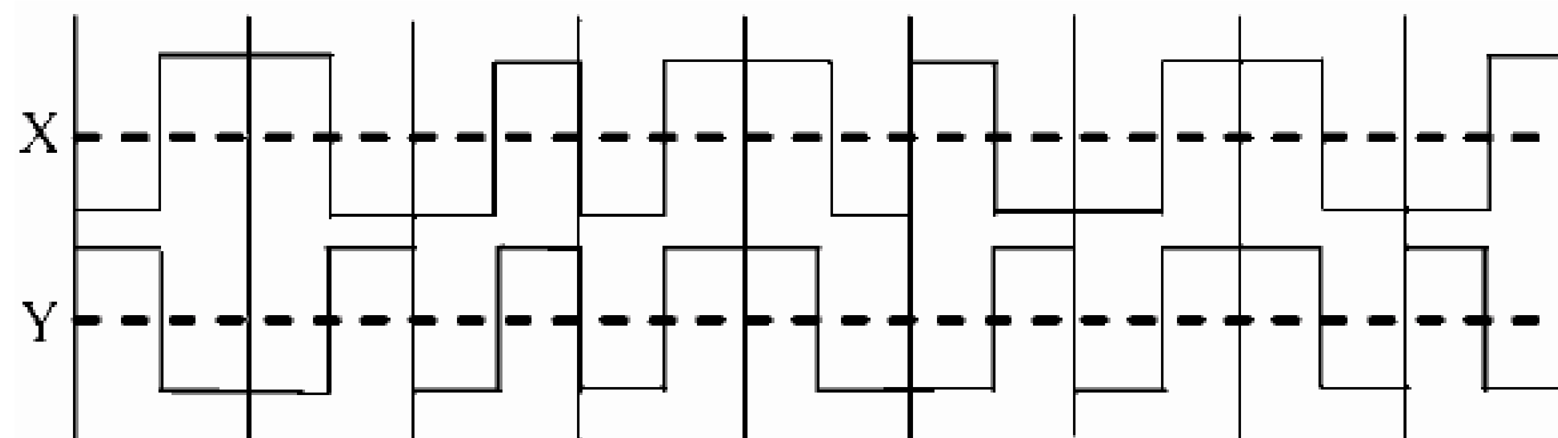
5 位二进制代码的状态共有 32 种，其中 1 的个数都不少于 2 个，这样就保证了传输的代码能提供足够多的同步信息。另外，还有 5B/6B、8B/10B 等编码方法，其原理是类似的。

**参考答案**

（13）A （14）C

**试题（15）、（16）**

下图表示了某个数据的两种编码，这两种编码分别是__（15）__，该数据是__（16）__。




（15）A．X 为差分曼彻斯特码，Y 为曼彻斯特码
B．X 为差分曼彻斯特码，Y 为双极性码
C．X 为曼彻斯特码，Y 为差分曼彻斯特码
D．X 为曼彻斯特码，Y 为不归零码

（16）A．010011110 B．010011010
C．011011010 D．010010010

**试题（15）、（16）分析**

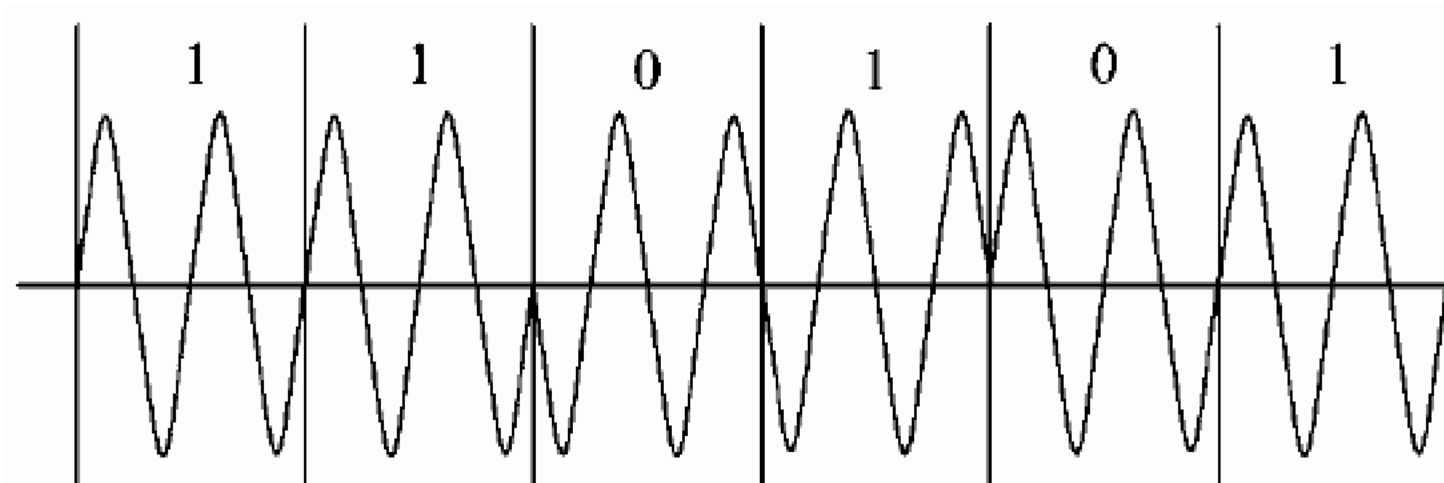
首先可以断定图中所示是两种双相码，然后按照曼彻斯特编码的特点（以正负或负正脉冲来区别“1”和“0”）和差分曼彻斯特编码的特点（以位前沿是否有电平跳变来区别“1”和“0”）可以断定，X 为曼彻斯特编码，Y 为差分曼彻斯特编码，表示的数据是 010011010。

**参考答案**

（15）C （16）B

**试题（17）、（18）**

下图所示的调制方式是__（17）__，若载波频率为 2400Hz，则码元速率为__（18）__。




（17）A. FSK　　B. 2DPSK　　C. ASK　　D. QAM

（18）A. 100 Baud　　B. 200 Baud　　C. 1200 Baud　　D. 2400 Baud

**试题（17）、（18）分析**

根据波形可以看出，这是一种差分编码，所以应选 2DPSK。另外，每一位包含两个周期，如果载波频率为 2400Hz，则码元速率就是 1200 波特。

**参考答案**

（17）B　（18）C

**试题（19）、（20）**

在相隔 2000km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发送到接收完数据需要的时间是__（19）__，如果用 50kb/s 的卫星信道传送，则需要的时间是__（20）__。

（19）A. 480ms　　B. 645ms　　C. 630ms　　D. 635ms

（20）A. 70ms　　B. 330ms　　C. 500ms　　D. 600ms

**试题（19）、（20）分析**

一个数据包从开始发送到接收完成的时间包含发送时间 $t_f$ 和传播延迟时间 $t_p$ 两部分，可以计算如下：

对电缆信道：$t_p$=2000km/(200km/ms)=10ms，$t_f$=3000b/4800b/s=625ms，$t_p+t_f$=635ms。

对卫星信道：$t_p$=270ms，$t_f$=3000b/50kb/s=60ms，$t_p+t_f$=270ms+60ms=330ms。

**参考答案**

（19）D　（20）B

**试题（21）**

对于选择重发 ARQ 协议，如果帧编号字段为 k 位，则窗口大小为__（21）__。

（21）A. $W \leqslant 2^k-1$　　B. $W \leqslant 2^{k-1}$　　C. $W=2^k$　　D. $W<2^{k-1}$

**试题（21）分析**

如果帧编号字段为 k 位，对于选择重发 ARQ 协议，发送窗口大小为 $W \leqslant 2^{k-1}$；对于后退 N 帧 ARQ 协议，则窗口大小为 $W \leqslant 2^k-1$。

**参考答案**

（21）B

**试题（22）、（23）**

RIPv2 对 RIPv1 协议有三方面的改进。下面的选项中，RIPv2 的特点不包括__（22）__。

在 RIPv2 中，可以采用水平分割法来消除路由循环，这种方法是指__（23）__。

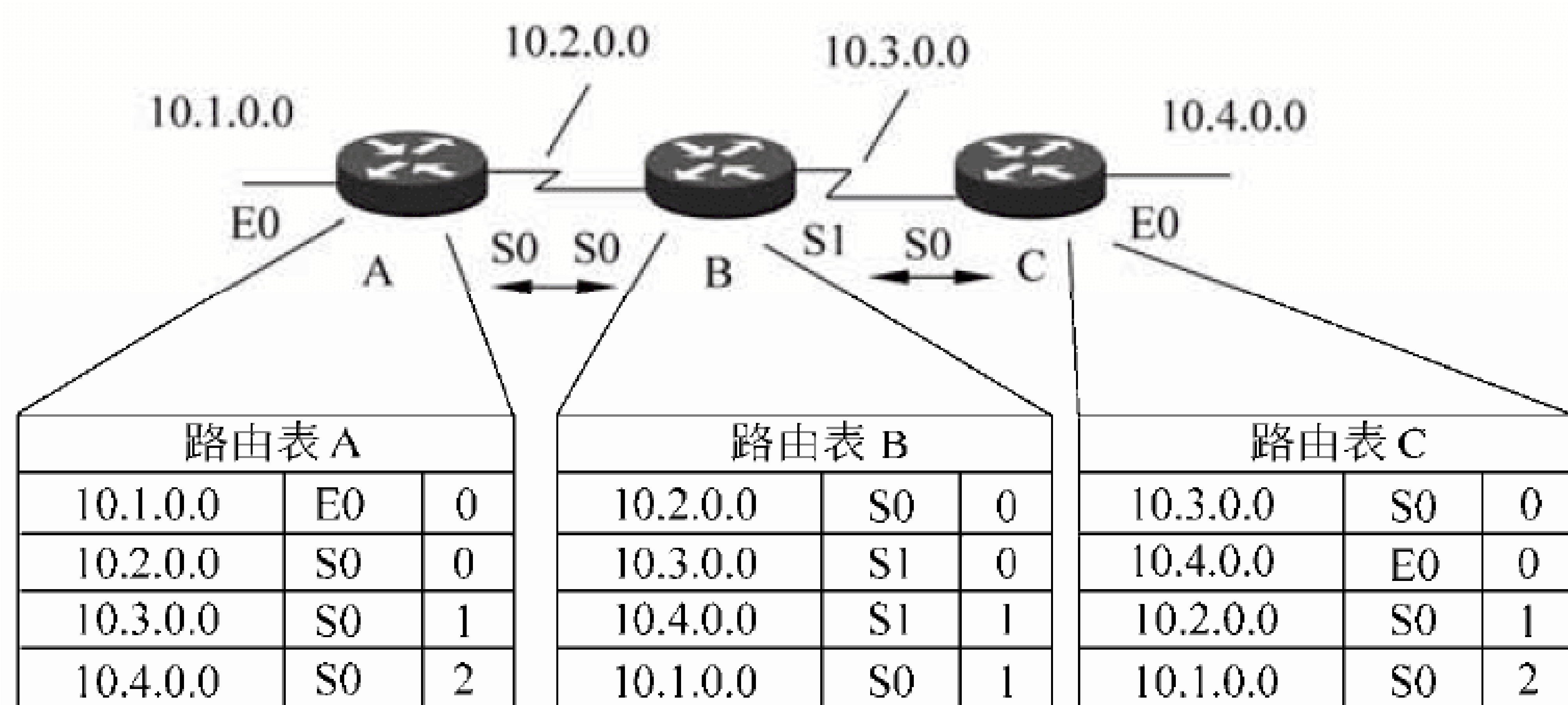
（22）A. 使用组播而不是广播来传播路由更新报文
　　B. 采用了触发更新机制来加速路由收敛
　　C. 使用经过散列的口令来限制路由信息的传播
　　D. 支持动态网络地址变换来使用私网地址

（23）A. 不能向自己的邻居发送路由信息
　　B. 不要把一条路由信息发送给该信息的来源
　　C. 路由信息只能发送给左右两边的路由器
　　D. 路由信息必须用组播而不是广播方式发送

**试题（22）、（23）分析**

RIPv2 是增强了的 RIP 协议，定义在 RFC 1721 和 RFC 1722（1994）中。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先，使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次，RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制路由更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

距离矢量算法要求相邻路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。




| 路由表 A | | |
|---|---|---|
| 10.1.0.0 | E0 | 0 |
| 10.2.0.0 | S0 | 0 |
| 10.3.0.0 | S0 | 1 |
| 10.4.0.0 | S0 | 2 |

| 路由表 B | | |
|---|---|---|
| 10.2.0.0 | S0 | 0 |
| 10.3.0.0 | S1 | 0 |
| 10.4.0.0 | S1 | 1 |
| 10.1.0.0 | S0 | 1 |

| 路由表 C | | |
|---|---|---|
| 10.3.0.0 | S0 | 0 |
| 10.4.0.0 | E0 | 0 |
| 10.2.0.0 | S0 | 1 |
| 10.1.0.0 | S0 | 2 |

例如在上图中，路由器 A、B、C 的路由表已经收敛，每个路由表的后两项是通过交换路由信息学习到的。如果在某一时刻，网络 10.4.0.0 发生故障，C 检测到故障，并通过接口 S0 把故障通知 B。然而，如果 B 在收到 C 的故障通知前将其路由表发送到 C，C 则会认为通过 B 可以访问 10.4.0.0，并据此将路由表中第二条记录修改为（10.4.0.0，S0，2）。这样一来，路由器 A、B、C 都认为通过其他的路由器存在一条通往 10.4.0.0 的

路径，结果导致目标地址为 10.4.0.0 的数据包在三个路由器之间来回传递，从而形成路由环路。

解决路由环路问题可以采用水平分割法（Split Horizon）。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图中 B 的路由表项加上一些注释，如下图所示，可以看出，每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。

| 路由表 B | | | |
|---|---|---|---|
| 10.2.0.0 | S0 | 0 | 不发送给 A |
| 10.3.0.0 | S1 | 0 | 不发送给 C |
| 10.4.0.0 | S1 | 1 | 不发送给 C |
| 10.1.0.0 | S0 | 1 | 不发送给 A |

简单的水平分割方案是："不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是："把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居"。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，前面提到的触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 C 在接收 B 的更新报文之前把网络 10.4.0.0 的故障告诉 B，则可以防止环路的形成。

**参考答案**

（22）D　（23）B

**试题（24）、（25）**

为了限制路由信息传播的范围，OSPF 协议把网络划分成 4 种区域（Area），其中 __(24)__ 的作用是连接各个区域的传输网络，__(25)__ 不接受本地自治系统以外的路由信息。

（24）A. 不完全存根区域　B. 标准区域　C. 主干区域　D. 存根区域

（25）A. 不完全存根区域　B. 标准区域　C. 主干区域　D. 存根区域

**试题（24）、（25）分析**

每个 OSPF 区域被指定了一个 32 位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为 0.0.0.0。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同。

- 标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。
- 主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。
- 存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。

- 完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。
- 不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（24）C　（25）D

**试题（26）**

MPLS 根据标记对分组进行交换，其标记中包含__（26）__。

（26）A．MAC 地址　　B．IP 地址

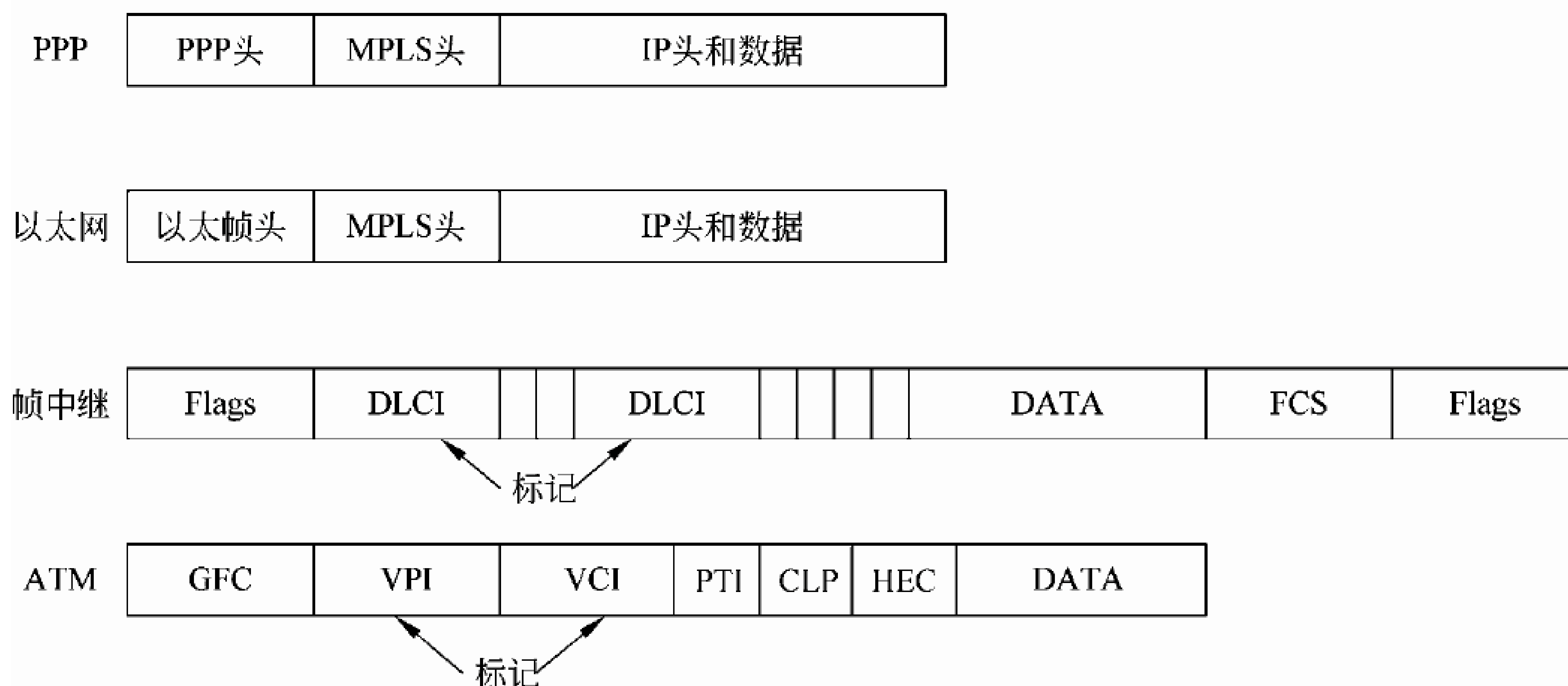
C．VLAN 编号　　D．分组长度

**试题（26）分析**

第三层交换是指利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换与路由不同，前者用硬件实现，速度快，而后者由软件实现，速度慢。三层交换机的工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住 MAC 层的目标地址和源地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧时就可以直接进行交换，不再调用路由功能。所以三层交换机不但具有路由功能，而且比通常的路由器转发的更快。



IETF 开发的多协议标记交换 MPLS（Multiprotocol Label Switching，RFC3031）把第二层的链路状态信息（带宽、延迟和利用率等）集成到第三层的协议数据单元中，从而简化和改进了第三层分组的交换过程。理论上，MPLS 支持任何第二层和第三层协议。MPLS 包头的位置界于第二层和第三层之间，可称为第 2.5 层，标准格式如上图所示。MPLS 承载的报文通常是 IP 包，当然也可以是以太帧、AAL5 包，甚至 ATM 信元等。可以承载 MPLS 的第二层协议可以是 PPP、以太帧、ATM 和帧中继等，参见下图。




当分组进入 MPLS 网络时，标记边缘路由器（Label Edge Router，LER）就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽和延迟等），而且还引用了 IP 头中的源地址字段、传输层端口号和服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路（Label Switch Path，LSP）中，标记交换路由器（Label Switch Router，LSR）将根据标记来处置分组，不再经过第三层转发，从而加快了网络的传输速度。

**参考答案**

（26）B

**试题（27）～（29）**

某 PC 不能接入 Internet，此时采用抓包工具捕获的以太网接口发出的信息如下：

| Source | Destination | Protocol | Info |
|---|---|---|---|
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254? Tell 213.127.115.31 |
| 213.127.115.31 | 213.127.115.255 | NBNS | Name query NB TRACKER9.BOL.BG<00> |
| 213.127.115.31 | 213.127.115.255 | NBNS | Name query NB BT.ROMMAN.NET<00> |
| 213.127.115.31 | 224.1.1.1 | UDP | Source port: ircu Destination port: ircu |
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254? Tell 213.127.115.31 |
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254? Tell 213.127.115.31 |

则该 PC 的 IP 地址为＿（27）＿，默认网关的 IP 地址为＿（28）＿。该 PC 不能接入 Internet 的原因可能是＿（29）＿。

（27）A．213.127.115.31　　B．213.127.115.255
　　C．213.127.115.254　　D．224.1.1.1

（28）A．213.127.115.31　　B．213.127.115.255
　　C．213.127.115.254　　D．224.1.1.1

（29）A．DNS 解析错误　　B．TCP/IP 协议安装错误
　　C．不能正常连接到网关　　D．DHCP 服务器工作不正常

**试题（27）～（29）分析**

采用抓包工具捕获的信息由源、目的、采用的协议以及数据报文中包含的信息组成。源字段中分别包含了该 PC 的 MAC 地址（QuantaCo_33:9b:be）和 IP 地址（213.127.115.31），其发出的信息表明主机不停地广播 ARP 报文，寻找网关 213.127.115.254。

由此，（27）、（28）选项中 A 为主机地址，B 选项 213.127.115.255 为广播地址，C 选项 213.127.115.254 为网关地址，D 选项 224.1.1.1 为组播地址。故（27）题选 A，（28）题选 C。

由主机不停地广播 ARP 报文寻找网关可以判断该 PC 不能接入 Internet 的原因是不能正常连接到网关，故（29）题选 C。

**参考答案**

（27）A （28）C （29）C

**试题（30）～（32）**

在 Linux 系统中，采用<u>（30）</u>命令查看进程输出的信息，得到下图所示的结果。系统启动时最先运行的进程是<u>（31）</u>，下列关于进程 xinetd 的说法中正确的是<u>（32）</u>。

| UID | PID | PPID | C | STIME | TTY | TIME | CMD |
|---|---|---|---|---|---|---|---|
| root | 1 | 0 | 0 | 10:10 | ? | 00:00:04 | init |
| root | 2 | 1 | 0 | 10:10 | ? | 00:00:00 | [keventd] |
| root | 3 | 1 | 0 | 10:10 | ? | 00:00:00 | [kapmd] |
| root | 4 | 1 | 0 | 10:10 | ? | 00:00:00 | [ksoftirqd_CPU0] |
| root | 9 | 1 | 0 | 10:10 | ? | 00:00:00 | [bdflush] |
| root | 5 | 1 | 0 | 10:10 | ? | 00:00:00 | [kswapd] |
| root | 6 | 1 | 0 | 10:10 | ? | 00:00:00 | [kscand/DMA] |
| root | 1720 | 1 | 0 | 10:11 | ? | 00:00:00 | xinetd -stayalive -reuse |
| root | 2074 | 2072 | 0 | 10:48 | pts/0 | 00:00:00 | bash |
| root | 2123 | 2074 | 0 | 11:03 | pts/0 | 00:00:00 | ps -aef |

（30）A. ps -all B. ps-aef C. ls-a D. ls -la

（31）A. 0 B. null C. init D. bash

（32）A. xinetd 是网络服务的守护进程 B. xinetd 是定时任务的守护进程
C. xinetd 进程负责配置网络接口 D. xinetd 进程负责启动网卡

**试题（30）～（32）分析**

本题考查 Linux 操作系统命令相关知识。

Linux 系统中用 ls 命令查看目录信息；用 ps 命令查看进程信息的命令。ps 命令的几个主要参数和含义解释如下：

- -A：将关于所有进程（除了会话导带和与终端无关的进程）的信息写到标准输出。
- -D：将关于所有进程（除会话导带）的信息写到标准输出。
- -E：将除内核进程以外所有进程的信息写到标准输出。

- -F：生成一个完整列表。

在 ps 命令显示的进程信息中，PID 是该进程的 ID，Linux 进程的 ID 一般是根据创建的先后顺序递增的。从图中可知，init 进程的 PID 是 1，它在系统启动时第一个动态创建。

xinetd 是一个守护（daemon）进程，Linux 把一些网络相关服务（如 FTP、HTTP 等）的监听端口全部由 xinetd 集中监听，当收到相应的客户端请求之后，xinetd 进程就临时启动相应服务并把相应端口移交给相应服务，客户端断开之后，相应的服务进程结束，xinetd 继续监听。

**参考答案**

（30）B　（31）C　（32）A

**试题（33）**

Linux 操作系统中，网络管理员可以通过修改__（33）__文件对 Web 服务器端口进行配置。

（33）A. inetd.conf　B. lilo.conf　C. httpd.conf　D. resolv.conf

**试题（33）分析**

本题考查 Linux 中 Web 服务器端口配置相关知识。

在 Linux 系统中，很多服务的配置数据都保存在相应的配置文件中（文件名一般为 server-name.conf）。

inet.conf 是/usr/sbin/inetd 的初始化文件，告诉/usr/sbin/inetd 所需要监听的 inet 服务及有关信息，主要的信息有服务名称、协议（tcp 或 udp）、标志（wait 或 nowait）、属主、真实服务程序全路径、真实服务程序名称及参数。lilo.conf 是 Linux 中多引导程序 lilo 的配置文件；resolv.conf 是 DNS 域名解析服务的配置文件。

httpd.conf 是 Linux 中 Apache Web 服务的配置文件，其中的 Listen 选项用于配置服务的 IP 地址和端口号。例如，.Listen 192.168.1.1:8080 指定 Web 服务的 IP 地址为 192.168.1.1，端口号为 8080。

**参考答案**

（33）C

**试题（34）**

在 Linux 操作系统中，存放用户账号加密口令的文件是__（34）__。

（34）A. /etc/sam　B. /etc/shadow　C. /etc/group　D. /etc/security

**试题（34）分析**

本题考查 Linux 用户账号密码的相关知识。

在 Linux 操作系统中，存放用户账号和密码的文件有两个：/etc/passwd 和/etc/shadow。/etc/shadow 文件是/etc/passwd 的影子文件，和/etc/passwd 应该是对应互补的。shadow 内容包括用户及被加密的密码以及其他/etc/passwd 不能包括的信息，比如用户的有效期限等。

**参考答案**

（34）B

**试题（35）、（36）**

在 Windows 中运行＿（35）＿命令后得到如下图所示的结果。如果要将目标地址为 102.217.112.0/24 的分组经 102.217.115.1 发出，需增加一条路由，正确的命令为＿（36）＿。

```
Active Routes:
Network Destination  Netmask          Gateway          Interface        Metric
  0.0.0.0            0.0.0.0          102.217.115.254  102.217.115.132  20
  127.0.0.0          255.0.0.0        127.0.0.1        127.0.0.1        1
  102.217.115.128    255.255.255.128  102.217.115.132  102.217.115.132  20
  102.217.115.132    255.255.255.255  127.0.0.1        127.0.0.1        20
  102.217.115.255    255.255.255.255  102.217.115.132  102.217.115.132  20
  224.0.0.0          240.0.0.0        102.217.115.132  102.217.115.132  20
  255.255.255.255    255.255.255.255  102.217.115.132  102.217.115.132  1
  255.255.255.255    255.255.255.255  102.217.115.132         2         1
Default Gateway:     102.217.115.254
```

（35）A．ipconfig /renew B．ping C．nslookup D．route print

（36）A．route add 102.217.112.0 mask 255.255.255.0 102.217.115.1

B．route add 102.217.112.0 255.255.255.0 102.217.115.1

C．add route 102.217.112.0 255.255.255.0 102.217.115.1

D．add route 102.217.112.0 mask 255.255.255.0 102.217.115.1

**试题（35）、（36）分析**

Route 在本地 IP 路由表中显示和修改条目。其语法为：

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric
Metric]] [if Interface]]
```

其中，命令参数 print 用于显示主机路由信息，add 用于添加路由，change 用于更改现存路由，delete 用于删除路由。

空（35）的选项中 ipconfig /renew 用于命令重新自动获取 IP 地址；ping 命令通过向对方主机发送“网际消息控制协议（ICMP）”回响请求消息来验证与对方计算机的连接，是用于检测网络连接性、可到达性的 TCP/IP 命令；nslookup 最简单的用法就是查询域名对应的 IP 地址，包括 A 记录和 CNAME 记录；route print 用于显示主机路由信息。故正确答案为 D。

Route 命令参数 add 用于添加路由，例如要添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1，跃点数为 7 的路由，正确的命令为：

```
route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7
```

故空（36）选择 A。

**参考答案**

（35）D （36）A

**试题（37）**

下列关于 Microsoft 管理控制台（MMC）的说法中，错误的是__（37）__。

（37）A．MMC 集成了用来管理网络、计算机、服务及其他系统组件的管理工具

B．MMC 创建、保存并打开管理工具单元

C．MMC 可以运行在 Windows XP 和 Windows 2000 操作系统上

D．MMC 是用来管理硬件、软件和 Windows 系统的网络组件

**试题（37）分析**

Microsoft 管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。可以使用 MMC 创建、保存并打开管理工具单元，这些管理工具用来管理软件、硬件和 Windows 系统的网络组件。MMC 可以运行在各种 Windows 9x/NT 操作系统上，以及 Windows XP Home Edition/XP Professional 和 Windows Server 2003 家族的操作系统上。

MMC 不执行管理功能，但集成管理工具。可以添加到控制台的主要工具类型称为管理单元，其他可添加的项目包括 ActiveX 控件、网页的链接、文件夹、任务板视图和任务。

但是，MMC 不是管理软件、硬件和 Windows 系统的网络组件，故（37）题选择 D。

**参考答案**

（37）D

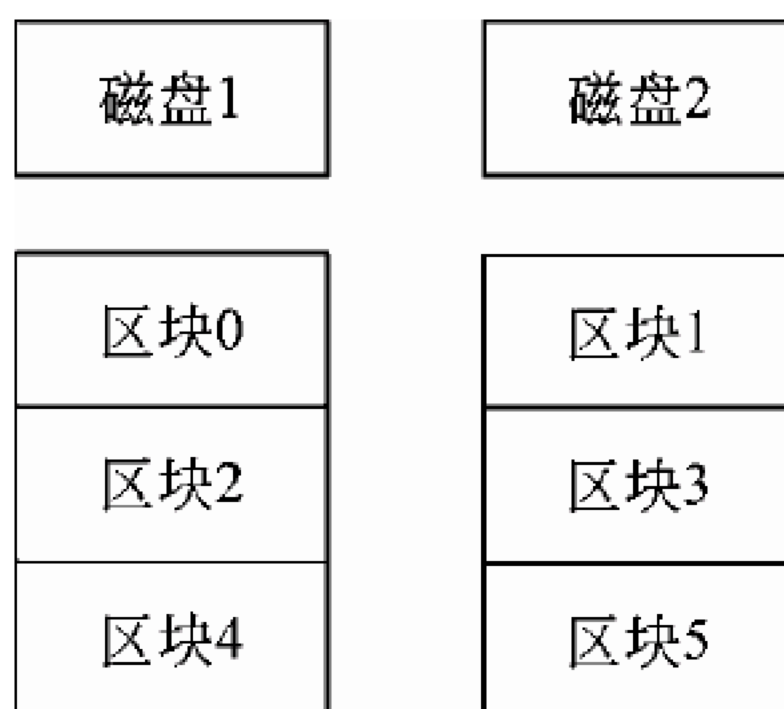
**试题（38）**

RAID 技术中，磁盘容量利用率最高的是__（38）__。

（38）A．RAID 0　　B．RAID 1　　C．RAID 3　　D．RAID 5

**试题（38）分析**

RAID 0 需要两个以上硬盘驱动器，每个磁盘划分为不同的区块，如下图所示。




数据按区块 A1、A2、A3、A4、…的顺序存储，数据访问采用交叉存取、并行传输的方式。将数据分布在不同驱动器上可以提高传输速度，平衡驱动器的负载。这种系统没有镜像盘，也没有差错控制措施，磁盘容量利用率在 RAID 技术中最高。

**参考答案**

（38）A

**试题（39）**

xDSL 技术中，能提供上下行信道非对称传输的是__（39）__。

（39）A．ADSL 和 HDSL　　B．ADSL 和 VDSL
　　　C．SDSL 和 VDSL　　D．SDSL 和 HDSL

**试题（39）分析**

数字用户线路（Digital Subscriber Line，DSL）允许用户在传统电话线上提供高速的数据传输，用户计算机借助于 DSL 调制解调器连接到电话线上，通过 DSL 连接访问互联网络或者企业网络。

DSL 技术存在多种类型，以下是常见的技术类型：

- ADSL：非对称 DSL，用户的上下行流量不对称，一般具有三个信道，分别为 1.544～9Mb/s 的高速下行信道，16～640kb/s 的双工信道，64kb/s 的语音信道。
- SDSL：对称 DSL，用户的上下行流量对等，最高可以达到 1.544Mb/s。
- HDSL：高比特率 DSL，是在两个线对上提供 1.544Mb/s 或在三个线对上提供 2.048Mb/s 对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为 3700～4600m。
- VDSL：甚高比特率 DSL，一种快速非对称 DSL 业务，可以在一对电话线上提供数据和语音业务。

**参考答案**

（39）B

**试题（40）**

若 FTP 服务器开启了匿名访问功能，匿名登录时需要输入的用户名是__（40）__。

（40）A．root　　B．user　　C．guest　　D．anonymous

**试题（40）分析**

FTP 服务器采用用户名 anonymous 进行匿名登录。

**参考答案**

（40）D

**试题（41）**

在 Kerberos 系统中，使用一次性密钥和__（41）__来防止重放攻击。

（41）A. 时间戳　　B. 数字签名　　C. 序列号　　D. 数字证书

**试题（41）分析**

本题考查 Kerberos 系统安全相关知识。

一次性密钥、序列号和时间戳都是对付重放攻击的有效手段，Kerberos 系统采用一次性密钥和时间戳来防止重放攻击。

**参考答案**

（41）A

**试题（42）**

在下面 4 种病毒中，__（42）__可以远程控制网络中的计算机。

（42）A． worm.Sasser.f　　B． Win32.CIH

C． Trojan.qq3344　　D． Macro.Melissa

**试题（42）分析**

本题考查病毒相关知识。

以上 4 种病毒中，worm 是蠕虫病毒，Win32.CIH 是 CIH 病毒，Macro.Melissa 是宏病毒，这三种病毒都属于单机病毒；而 Trojan.qq3344 是一种特洛伊木马，通过网络实现对计算机的远程攻击。

**参考答案**

（42）C

**试题（43）**

将 ACL 应用到路由器接口的命令是__（43）__。

（43）A． Router(config-if)#ip access-group 10 out

B． Router(config-if)#apply access-list 10 out

C． Router(config-if)#fixup access-list 10 out

D． Router(config-if)#route access-group 10 out

**试题（43）分析**

本题考查路由器配置命令，属于记忆题。

**参考答案**

（43）A

**试题（44）～（46）**

某网站向 CA 申请了数字证书，用户通过__（44）__来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过__（45）__进行加密和验证，该网站通过__（46）__进行解密和签名。

（44）A. CA 的签名　B. 证书中的公钥　C. 网站的私钥　D. 用户的公钥

（45）A. CA 的签名　B. 证书中的公钥　C. 网站的私钥　D. 用户的公钥

（46）A. CA 的签名　B. 证书中的公钥　C. 网站的私钥　D. 用户的公钥

**试题（44）～（46）分析**

本题考查数字证书相关知识点。

数字证书是由权威机构——CA 证书授权（Certificate Authority）中心发行的，能提供在 Internet 上进行身份验证的一种权威性电子文档，人们可以在因特网交往中用它来证明自己的身份和识别对方的身份。

数字证书包含版本、序列号、签名算法标识符、签发人姓名、有效期、主体名和主体公钥信息等并附有 CA 的签名，用户获取网站的数字证书后通过验证 CA 的签名来确

认数字证书的有效性，从而验证网站的真伪。

在用户与网站进行安全通信时，用户发送数据时使用网站的公钥（从数字证书中获得）加密，收到数据时使用网站的公钥验证网站的数字签名；网站利用自身的私钥对发送的消息签名和对收到的消息解密。

**参考答案**

（44）A　（45）B　（46）C

**试题（47）**

IPSec 的加密和认证过程中所使用的密钥由__（47）__机制来生成和分发。

（47）A．ESP　B．IKE　C．TGS　D．AH

**试题（47）分析**

本题考查 IPSec 相关知识。

IPSec 密钥管理利用 IKE（Internet 密钥交换协议）机制实现， IKE 解决了在不安全的网络环境（如 Internet）中安全地建立或更新共享密钥的问题。

**参考答案**

（47）B

**试题（48）**

SSL 协议使用的默认端口是__（48）__。

（48）A．80　B．445　C．8080　D．443

**试题（48）分析**

本题属于记忆题。

80 端口是 Web 服务默认端口；8080 端口一般用于局域网内部提供 Web 服务；445 端口和 139 端口一样，用于局域网中共享文件夹或共享打印机。

**参考答案**

（48）D

**试题（49）、（50）**

某用户分配的网络地址为 192.24.0.0～192.24.7.0，这个地址块可以用__（49）__表示，其中可以分配__（50）__个主机地址。

（49）A．192.24.0.0/20　B．192.24.0.0/21

C．192.24.0.0/16　D．192.24.0.0/24

（50）A．2032　B．2048　C．2000　D．2056

**试题（49）、（50）分析**

192.24.0.0 的二进制表示为：　**11000000 00011000 00000** 000 00000000

192.24.7.0 的二进制表示为：　**11000000 00011000 00000** 111 00000000

汇聚后的网络地址为 **11000000 00011000 00000** 000 00000000，即 192.24.0.0/21。

可以分配的主机地址为 8×（$2^8$–2）＝2032。

**参考答案**

（49）B　（50）A

**试题（51）**

使用 CIDR 技术把 4 个 C 类网络 220.117.12.0/24、220.117.13.0/24、220.117.14.0/24 和 220.117.15.0/24 汇聚成一个超网，得到的地址是__（51）__。

（51）A．220.117.8.0/22　　B．220.117.12.0/22
C．220.117.8.0/21　　D．220.117.12.0/21

**试题（51）分析**

CIDR 技术是把小的网络汇聚成大的超网。这里 4 个网络地址的二进制表示如下：

220.117.12.0/24 的二进制表示为：　**11011100 01110101 00001100** 00000000
220.117.13.0/24 的二进制表示为：　**11011100 01110101 00001101** 00000000
220.117.14.0/24 的二进制表示为：　**11011100 01110101 00001110** 00000000
220.117.15.0/24 的二进制表示为：　**11011100 01110101 00001111** 00000000

可以看出，汇聚后的网络地址为 **11011100 01110101 000011**00 00000000，即 220.117.12.0/22。

**参考答案**

（51）B

**试题（52）**

某公司网络的地址是 200.16.192.0/18，划分成 16 个子网，下面的选项中，不属于这 16 个子网地址的是__（52）__。

（52）A．200.16.236.0/22　　B．200.16.224.0/22
C．200.16.208.0/22　　D．200.16.254.0/22

**试题（52）分析**

地址 200.16.192.0/18 的二进制表示为 **11001000.00010000.11**000000.00000000，将其划分为 16 个子网，则各个子网的地址为：

**11001000.00010000.110000**00.00000000——200.16.192.0/22
**11001000.00010000.110001**00.00000000——200.16.196.0/22
**11001000.00010000.110010**00.00000000——200.16.200.0/22
**11001000.00010000.110011**00.00000000——200.16.204.0/22
**11001000.00010000.110100**00.00000000——200.16.208.0/22
**11001000.00010000.110101**00.00000000——200.16.212.0/22
**11001000.00010000.110110**00.00000000——200.16.216.0/22
**11001000.00010000.110111**00.00000000——200.16.220.0/22
**11001000.00010000.111000**00.00000000——200.16.224.0/22
**11001000.00010000.111001**00.00000000——200.16.228.0/22
**11001000.00010000.111010**00.00000000——200.16.232.0/22
**11001000.00010000.111011**00.00000000——200.16.236.0/22

**11001000.00010000.111100**00.00000000——200.16.240.0/22

**11001000.00010000.111101**00.00000000——200.16.244.0/22

**11001000.00010000.111110**00.00000000——200.16.248.0/22

**11001000.00010000.111111**00.00000000——200.16.252.0/22

可以看出，以上 16 个网络地址的第三个字节都能被 4 整除，而答案 D 中的 254 不能被 4 整除。

**参考答案**

（52）D

**试题（53）**

IPv6 地址 12AB:0000:0000:CD30:0000:0000:0000:0000/60 可以表示成各种简写形式，下面的选项中，写法正确的是__（53）__。

（53）A．12AB:0:0:CD30::/60　　　　B．12AB:0:0:CD3/60

C．12AB::CD30/60　　　　D．12AB::CD3/60

**试题（53）分析**

IPv6 地址采用冒号分隔的十六进制数表示，例如下面是一个 IPv6 地址

```
8000:0000:0000:0000:0123:4567:89AB:CDEF
```

为了便于书写，规定了一些简化写法。首先，每个字段前面的 0 可以省去，例如 0123 可以简写为 123；其次，一个或多个全 0 字段 0000 可以用一对冒号代替。例如以上地址可简写为：

```
8000::123:4567:89AB:CDEF
```

IPv6 地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可表示为“IPv6 地址/前缀长度”的形式。例如，60 位的地址前缀 12AB00000000CD3 有下列几种合法的表示形式：

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60
```

下面的表示形式是不合法的：

```
12AB:0:0:CD3/60 （在 16 位的字段中可以省掉前面的 0，不能省掉后面的 0）
12AB::CD30/60（可展开为 12AB:0000:0000:0000:0000:0000:0000:CD30）
12AB::CD3/60（可展开为 12AB:0000:0000:0000:0000:0000:0000:0CD3）
```

一般来说，结点地址与其子网前缀组合起来可采用紧缩形式表示，例如结点地址

```
12AB:0:0:CD30:123:4567:89AB:CDEF
```

若其子网号为12AB:0:0:CD30::/60，则等价的写法是

```
12AB:0:0:CD30:123:4567:89AB:CDEF/60
```

**参考答案**

（53）A

**试题（54）、（55）**

IPv6 协议数据单元由一个固定头部和若干个扩展头部以及上层协议提供的负载组成，其中用于表示松散源路由功能的扩展头是__（54）__。如果有多个扩展头部，第一个扩展头部为__（55）__。

（54）A. 目标头部　　B. 路由选择头部
　　　C. 分段头部　　D. 安全封装负荷头部

（55）A. 逐跳头部　　B. 路由选择头部
　　　C. 分段头部　　D. 认证头部

**试题（54）、（55）分析**

IPv6 有 6 种扩展头部，如下表所示，这 6 种扩展头部都是任选的。扩展头部的作用是保留 IPv4 某些字段的功能，但只是由特定的网络设备来检查处理，而不是每个设备都要处理。

<table>
<tr><th>头 部 名 称</th><th colspan="2">解　　释</th></tr>
<tr><td rowspan="2">逐跳选项（hop-by-hop option）</td><td rowspan="2">这些信息由沿途各个路由器处理</td><td>特大净负荷<br>Jumbograms</td></tr>
<tr><td>路由器警戒<br>Router Alert</td></tr>
<tr><td>目标选项（Destination option）</td><td colspan="2">选项中的信息由目标结点检查处理</td></tr>
<tr><td>路由选择（routing）</td><td colspan="2">给出一个路由器地址列表组成，类似于 IPv4 的松散源路由和路由记录</td></tr>
<tr><td>分段（Fragmentation）</td><td colspan="2">处理数据报的分段问题</td></tr>
<tr><td>认证（Authentication）</td><td colspan="2">由接收者进行身份认证</td></tr>
<tr><td>封装安全负荷(Encrypted security payload)</td><td colspan="2">对分组内容进行加密的有关信息</td></tr>
</table>

如果一个 IPv6 分组包含多个扩展头，建议采用下面的封装顺序：

（1）IPv6 头部。

（2）逐跳选项头。

（3）目标选项头（IPv6 头部目标地址字段中指明的第一个目标结点要处理的信息，以及路由选择头中列出的后续目标结点要处理的信息）。

（4）路由选择头。

（5）分段头。

（6）认证头。

（7）封装安全负荷头。

（8）目标选项头（最后的目标结点要处理的信息）。

（9）上层协议头部。

**参考答案**

（54）B　（55）A

**试题（56）**

下面关于帧中继网络的描述中，错误的是__（56）__。

（56）A. 用户的数据速率可以在一定的范围内变化

B. 既可以适应流式业务，又可以适应突发式业务

C. 帧中继网可以提供永久虚电路和交换虚电路

D. 帧中继虚电路建立在 HDLC 协议之上

**试题（56）分析**

帧中继（FR）在第二层建立虚电路，用帧方式承载数据业务，因而第三层被简化掉了。在用户平面，FR 帧比 HDLC 帧操作简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。

FR 的虚电路分为永久虚电路（Permanent Virtual Circuit，PVC）和交换虚电路（Switch Virtual Circuit，SVC）。PVC 是在两个端用户之间建立的固定逻辑连接，为用户提供约定的服务。帧中继交换设备根据预先配置的虚电路表把数据帧从一段链路交换到另外一段链路，最终传送到接收用户。SVC 是通过 ISDN 信令协议（Q931/ Q933）临时建立的逻辑信道，它以呼叫的形式建立和释放连接。很多帧中继网络只提供 PVC 业务，不提供 SVC 业务。

帧中继网为用户提供约定信息速率（CIR）和扩展的信息速率（EIR），以及约定突发量（Bc）和超突发量（Be），这些参数之间有如下关系：

- Bc = Tc×CIR
- Be = Tc×EIR

其中，Tc 为数据速率测量时间。网络应该保证用户以等于或低于 CIR 的速率传送数据。对于超过 CIR 的 Bc 部分，在正常情况下能可靠地传送，但若出现网络拥塞，则会被优先丢弃。对于 Be 部分的数据，网络将尽量传送，但不保证传送成功。对于超过 Bc+Be 的部分，网络拒绝接收。这是在保证用户正常通信的前提下防止网络拥塞的主要手段，对各种数据通信业务有很强的适应能力。

在帧中继网中，用户的信息速率可以在一定的范围内变化，从而既可以适应流式业务，又可以适应突发式业务。

**参考答案**

（56）D

**试题（57）**

SNMP MIB 中被管对象的 Access 属性不包括__（57）__。

（57）A. 只读　　B. 只写　　C. 可读写　　D. 可执行

**试题（57）分析**

SNMP MIB 中被管对象的 Access 包括读、写、可读写属性，但不包括可执行。

**参考答案**

（57）D

**试题（58）**

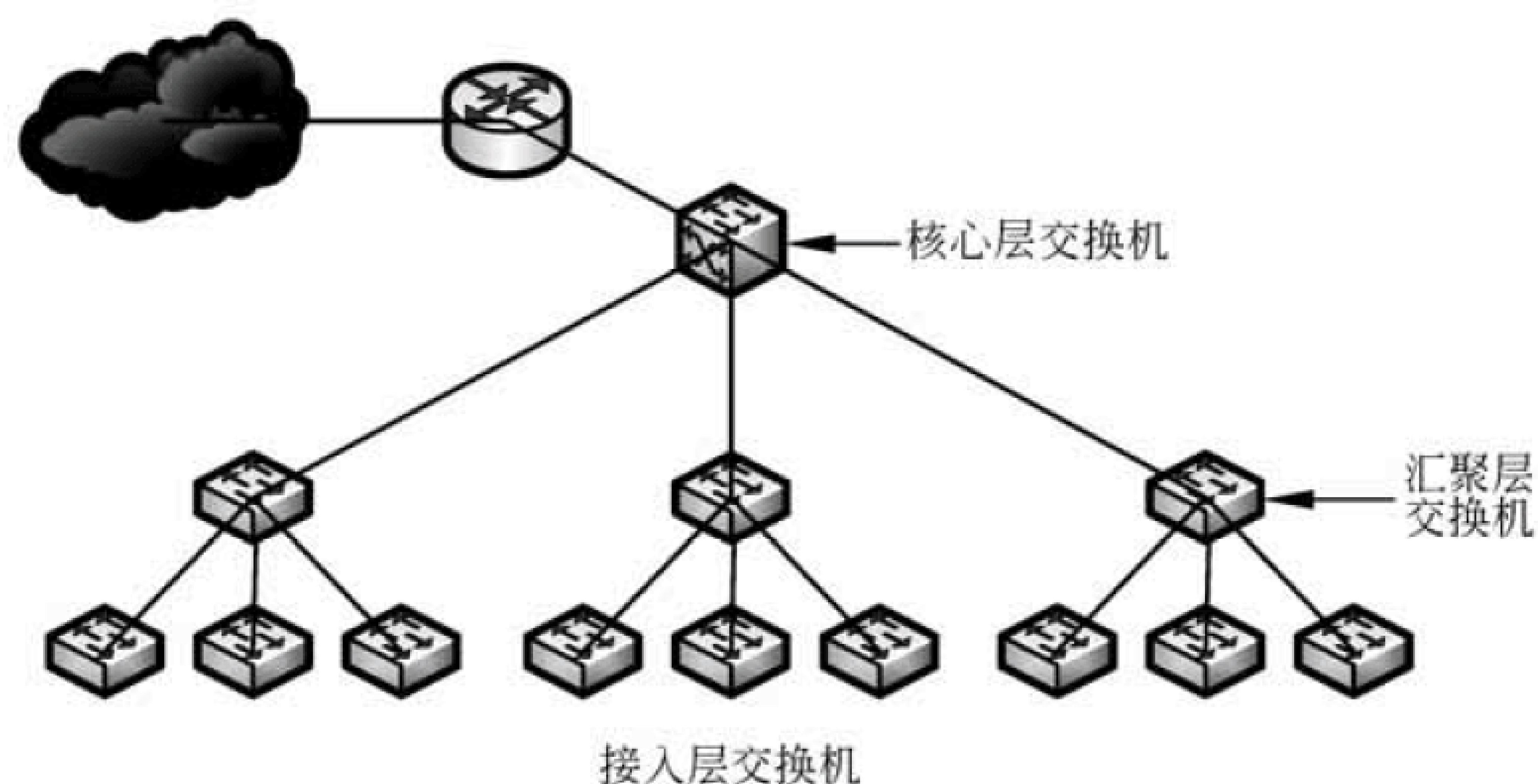
汇聚层交换机应该实现多种功能，下面选项中，不属于汇聚层功能的是__（58）__。

（58）A. VLAN 间的路由选择　　B. 用户访问控制

C. 分组过滤　　D. 组播管理

**试题（58）分析**

网络的分层结构把复杂的大型网络分解为多个容易管理的小型网络，每一层交换设备分别实现不同的特定任务。分层的网络设计如下图所示。




- 接入层交换机：接入层是工作站连接网络的入口，实现用户的访问控制，这一层的交换机应该以低成本提供高密度的接入端口。例如，Cisco Catalyst 2950 系列可以提供 12 或 24 个快速以太网端口，适合中小型企业网络使用。
- 汇聚层交换机：汇聚层将网络划分为多个广播/组播域，可以实现 VLAN 间的路由选择，并通过访问控制列表实现分组过滤。这一层交换机的端口数量和交换速率不要求很高，但应提供第三层交换功能。例如，Cisco Catalyst 3550 系列交换机具有多个 10M/100M 端口和两个内置的千兆以太网端口，可以支持多种 GBIC 收发器，同时提供先进的服务质量（QoS）和速度限制，以及安全访问控制列表、组播管理和高性能的 IP 路由。
- 核心层交换机：核心层应采用可扩展的高性能交换机组成园区网的主干线路，提供链路冗余、路由冗余、VLAN 中继和负载均衡等功能，并且与汇聚层交换机具

有兼容的技术，支持相同协议。例如，Cisco Catalyst 6500 系列交换机就是一种适合部署到核心网络的交换机。

**参考答案**

（58）B

**试题（59）**

交换机命令 Switch >enable 的作用是__（59）__。

（59）A. 配置访问口令　　B. 进入配置模式

C. 进入特权模式　　D. 显示当前模式

**试题（59）分析**

交换机的命令状态如下：

- Switch >：交换机处于用户命令状态，这时用户可以看交换机的连接状态，访问其他网络和主机，但不能看到和更改交换机配置的内容。
- Switch #：在 Switch >提示符下输入 enable，交换机进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改交换机的配置内容。
- Switch (config)#：在 Switch #提示符下输入 configure terminal，这时交换机处于全局配置状态，可以配置交换机的全局参数。
- Switch (config-if)#：交换机处于局部配置状态，这时可以配置交换机当前端口的参数。

**参考答案**

（59）C

**试题（60）**

IEEE 802.1q 协议的作用是__（60）__。

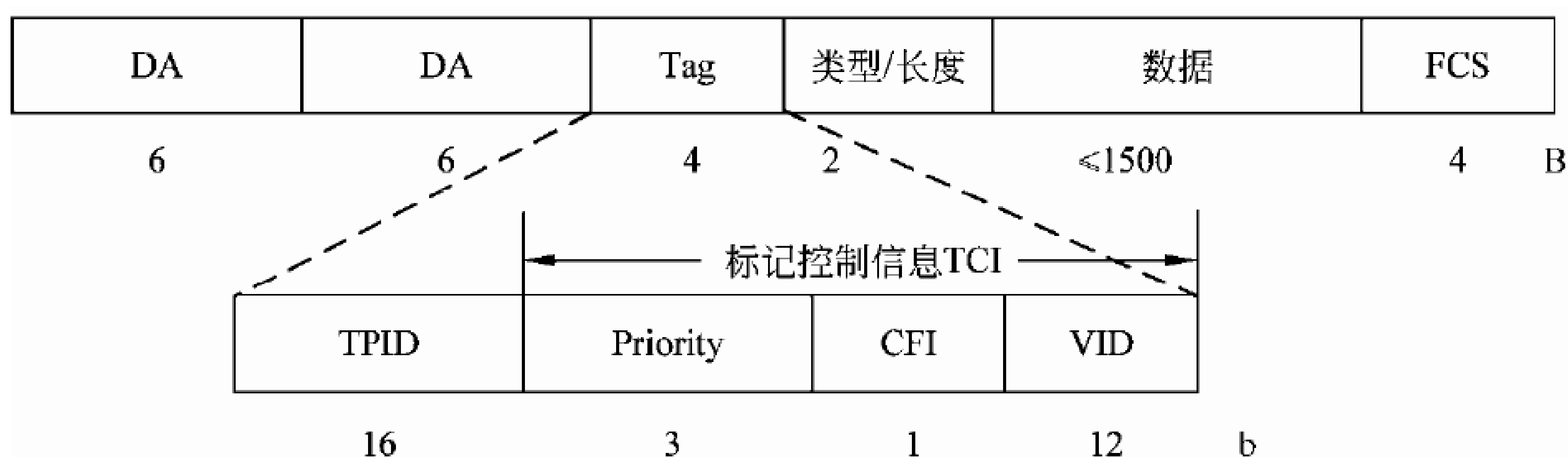
（60）A. 生成树协议　　B. 以太网流量控制

C. 生成 VLAN 标记　　D. 基于端口的认证

**试题（60）分析**

在划分成 VLAN 的局域网中，每个数据包都被加上一个有关 VALN 属性的帧标记，交换机之间根据帧标记来转发数据包。一个 VLAN 可以跨越多个交换机，带有 VLAN 标记的数据包在交换机之间的中继链路上传播，在进入 PC 时恢复原来的帧格式。

VLAN 帧标记有两种格式：一种是交换机间链路协议（Inter-Switch Link，ISL），这是 Cisco 公司的专利协议，适用于 Cisco 的 Catalyst 系列交换机；另一种是 IEEE 802.1q 协议，是在原来的以太帧中增加了 4 个字节的标记（Tag）字段，如下图所示，其中标记控制信息（Tag Control Information，TCI ）包含 Priority、CFI 和 VID 三部分，各个字段的含义参见下图。




802.1q 并没有定义优先级的含义，提供这种功能的是 802.1p 协议。另外，802.1p 协议还提供了组播过滤机制，以配合 IP 组播功能，使得 IP 组播流量不会被交换机广播扩散。许多高档交换机都把实现 802.1p 和 802.1q 作为重要的性能指标。

**参考答案**

（60）C

**试题（61）**

CSMA/CD 协议可以利用多种监听算法来减小发送冲突的概率，下面关于各种监听算法的描述中，正确的是__（61）__。

（61）A. 非坚持型监听算法有利于减少网络空闲时间

B. 1-坚持型监听算法有利于减少冲突的概率

C. P-坚持型监听算法无法减少网络的空闲时间

D. 坚持型监听算法能够及时抢占信道

**试题（61）分析**

CSMA/CD 协议定义的监听算法有以下三种：

（1）非坚持型监听算法。当一个站准备好帧，发送之前先监听信道：

① 若信道空闲，立即发送，否则转②。

② 若信道忙，则后退一个随机时间，重复①。

由于随机时延后退，从而减少了冲突的概率。然而，可能出现的问题是因为后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

（2）1-坚持型监听算法。当一个站准备好帧，发送之前先监听信道：

① 若信道空闲，立即发送，否则转②。

② 若信道忙，继续监听，直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

（3）P-坚持型监听算法。这种算法汲取了以上两种算法的优点，但较为复杂。

① 若信道空闲，以概率 P 发送，以概率（1-P）延迟一个时间单位。一个时间单位等于网络传输时延τ。

② 若信道忙，继续监听直到信道空闲，转①。

③ 如果发送延迟一个时间单位τ，则重复①。

困难的问题是决定概率 P 的值，P 的取值应在重负载下能使网络有效地工作。为了

说明 P 的取值对网络性能的影响，假设有 n 个站正在等待发送，与此同时，有一个站正在发送。当这个站发送停止时，实际要发送的站数等于 nP。若 nP 大于 1，则必有多个站同时发送，这必然会发生冲突，nP 必须小于 1。然而若 P 值太小，发送站就要等待较长的时间，在轻负载的情况下，这意味着较大的发送时延。

**参考答案**

（61）D

**试题（62）**

在 Windows 的 DoS 窗口中键入命令

```
C:\> nslookup
set type=ptr
> 211.151.91.165
```

这个命令序列的作用是__（62）__。

（62）A. 查询 211.151.91.165 的邮件服务器信息
B. 查询 211.151.91.165 到域名的映射
C. 查询 211.151.91.165 的资源记录类型
D. 显示 211.151.91.165 中各种可用的信息资源记录

**试题（62）分析**

Nslookup 显示可用来诊断域名系统（DNS）基础结构的信息。只有在已安装 TCP/IP 协议的情况下才可以使用 Nslookup 命令行工具。Nslookup 有两种模式：交互式和非交互式。语法为：

```
nslookup [-option] [hostname] [server]
```

在交互模式下，部分查询类型和查询的内容如下：

- set type=mx：查询邮件交换记录；
- set type=soa：查询 SOA（Start of Authority）记录；
- set type=CNAME：查询别名记录；
- set type=NS：查询名字服务器记录；
- set type=PTR：查询反向记录（从 IP 地址解释域名）。

**参考答案**

（62）B

**试题（63）**

在 Windows 的命令窗口中键入命令 arp -s 10.0.0.80 00-AA-00-4F-2A-9C，这个命令的作用是__（63）__。

（63）A. 在 ARP 表中添加一个动态表项　　B. 在 ARP 表中添加一个静态表项
C. 在 ARP 表中删除一个表项　　D. 在 ARP 表中修改一个表项

**试题（63）分析**

Arp 命令用于显示和修改地址解析协议（ARP）缓存表的内容，缓存表项是 IP 地址

与网卡地址对。计算机上安装的每个网卡各有一个缓存表。如果使用不含参数的 arp 命令，则显示帮助信息。Arp 命令的语法如下：

```
arp [-a  [InetAddr]  [-N IfaceAddr]]  [-g  [InetAddr]  [-N IfaceAddr]]
[-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
```

对以上命令参数解释如下：

- *-a* [*InetAddr*] [*-N IfaceAddr*]：显示所有接口的 ARP 缓存表。如果要显示特定 IP 地址的 ARP 表项，则使用参数 InetAddr；如果要显示指定接口的 ARP 缓存表，则使用参数-N IfaceAddr。这里，N 必须大写。InetAddr 和 IfaceAddr 都是 IP 地址。
- *-g* [*InetAddr] [-N IfaceAddr*]：与参数-a 相同。
- *-d InetAddr* [ *IfaceAddr* ]：删除由 InetAddr 指示的 ARP 缓存表项。要删除特定接口的 ARP 缓存表项，使用参数 IfaceAddr 指明接口的 IP 地址。要删除所有 ARP 缓存表项，使用通配符“*”代替参数 InetAddr。
- *-s InetAddr EtherAddr* [ *IfaceAddr*]：添加一个静态的 ARP 表项，把 IP 地址 InetAddr 解析为物理地址 EtherAddr。参数 IfaceAddr 指定了接口的 IP 地址。

用参数-s 添加的 ARP 表项是静态的，不会由于超时而被删除。如果 TCP/IP 协议停止运行，ARP 表项都被删除。为了生成一个固定的静态表项，可以在批文件中加入适当的 ARP 命令，并在机器启动时运行批文件。

要添加一个静态表项，把 IP 地址 10.0.0.80 解析为物理地址 00-AA-00-4F-2A-9C，则输入：

```
arp -s 10.0.0.80 00-AA-00-4F-2A-9C
```

下图是使用 arp 命令添加一个静态表项的例子。

```
C:\Documents and Settings\Administrator>arp -a

Interface: 100.100.17.17 --- 0x10003
  Internet Address      Physical Address      Type
  100.100.17.254        00-0f-e2-29-31-c1     dynamic

C:\Documents and Settings\Administrator>arp -s 202.117.17.254 00-1c-4f-52-2a-8c

C:\Documents and Settings\Administrator>arp -a

Interface: 100.100.17.17 --- 0x10003
  Internet Address      Physical Address      Type
  100.100.17.72         00-1e-8c-ad-f9-ce     dynamic
  100.100.17.75         00-40-d0-53-bf-86     dynamic
  100.100.17.254        00-0f-e2-29-31-c1     dynamic
  202.117.17.254        00-1c-4f-52-2a-8c     static
```

**参考答案**

（63）B

**试题（64）**

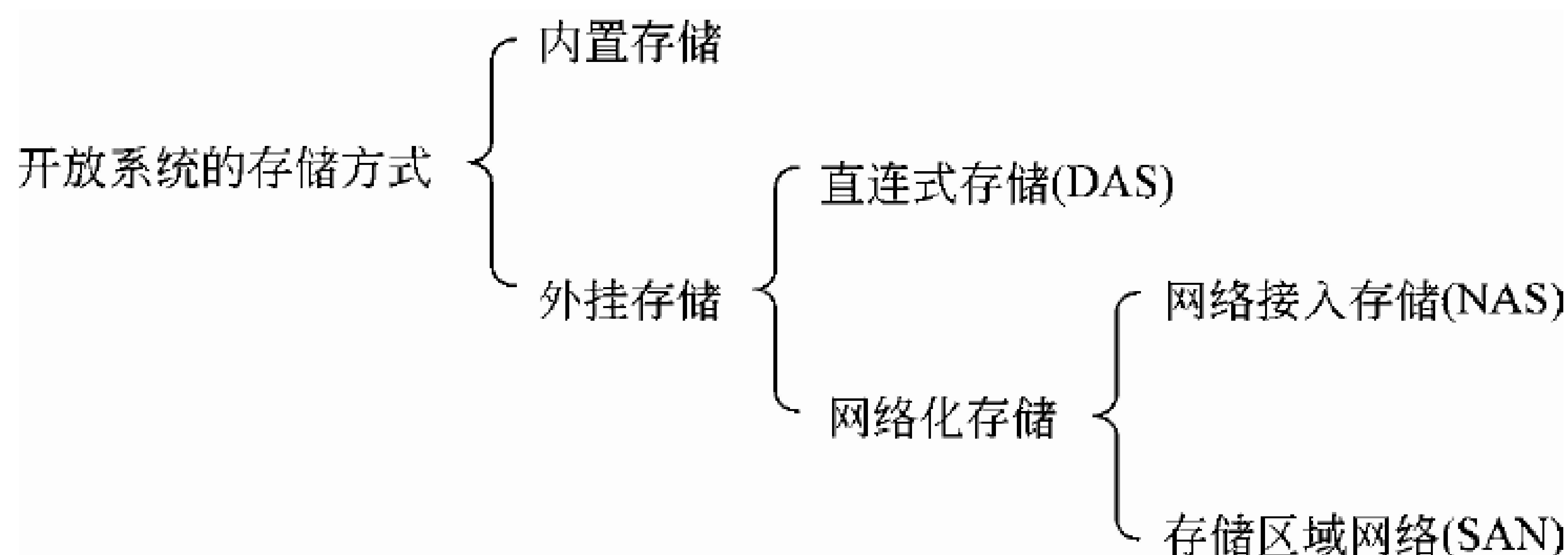
开放系统的数据存储有多种方式，属于网络化存储的是__（64）__。

（64）A. 内置式存储和 DAS　　B. DAS 和 NAS

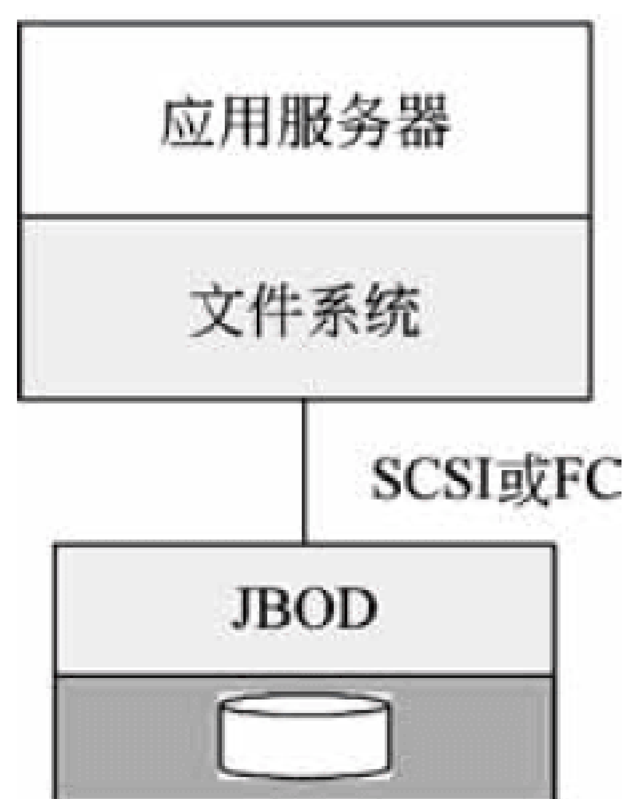
C. DAS 和 SAN　　D. NAS 和 SAN

**试题（64）分析**

基于 Windows、Linux 和 UNIX 等操作系统的服务器称为开放系统。开放系统的数据存储方式分为内置存储和外挂存储两种，而外挂存储又根据连接的方式分为直连式存储和网络化存储，目前应用的网络化存储方式有两种，即网络接入存储和存储区域网络，如下图所示。



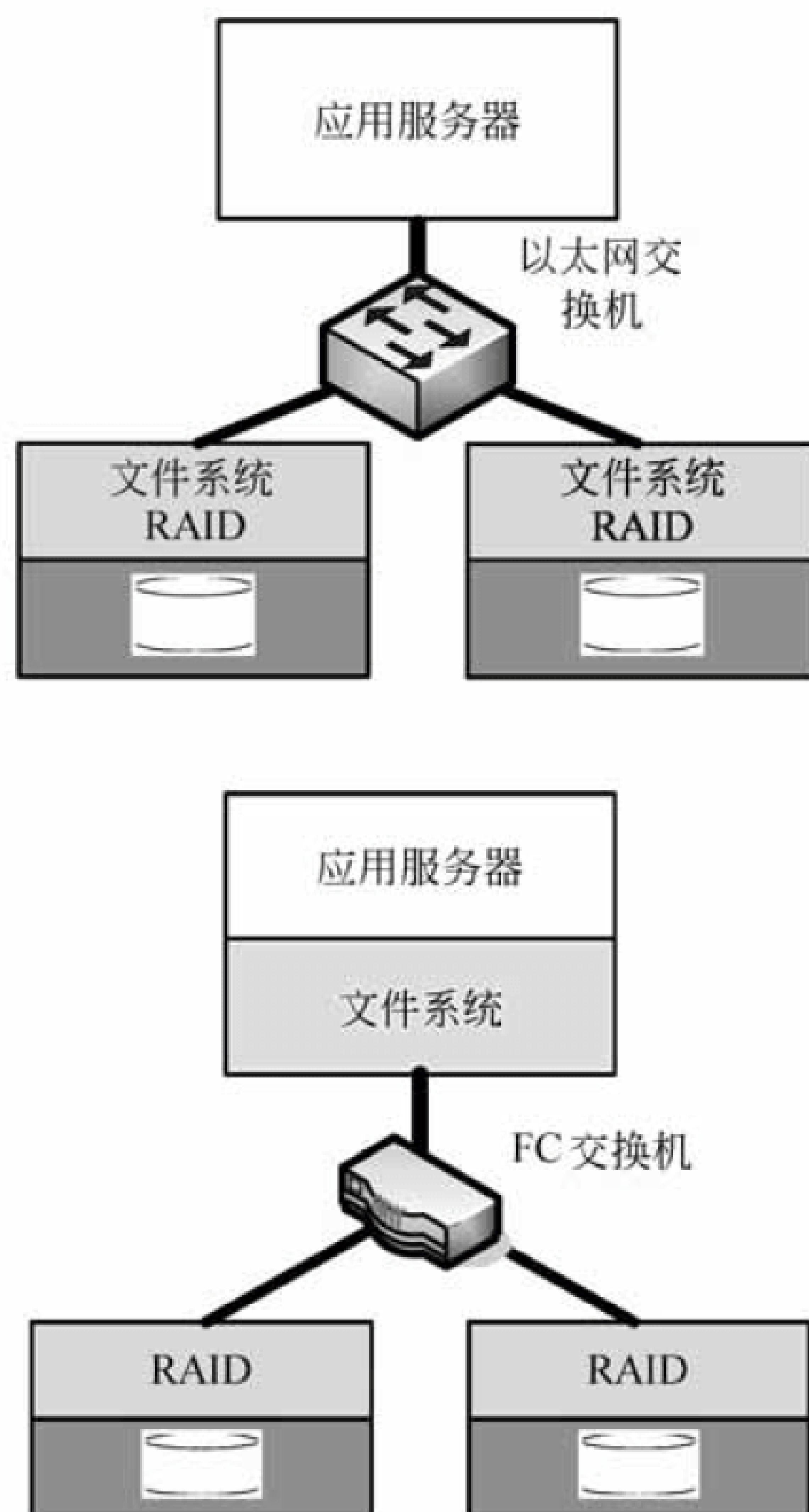

开放系统的直连式存储（Direct-Attached Storage，DAS）如下图所示，即在服务器上外挂了一组大容量硬盘，存储设备与服务器主机之间采用 SCSI 通道连接，带宽为 10MB/s、20MB/s、40MB/s 和 80MB/s 等。DAS 已经有近 40 年的使用历史，目前正在让位于日渐兴盛的网络化存储。




网络接入存储（Network Attached Storage，NAS）是将存储设备连接到现有的网络上，来提供数据存储和文件访问服务的设备。NAS服务器是在专用主机上安装简化了的瘦操作系统的文件服务器。NAS 服务器内置了与网络连接所需要的协议，可以直接联网，具有权限的用户都可以通过网络来访问 NAS 服务器中的文件。NAS 服务器直接连接磁盘阵列，它具备磁盘阵列的所有特征：高容量、高效能、高可靠性。典型的 NAS 都连接到普通的以太网上，提供预先配置好的磁盘容量和存储管理软件，成为完备的网络存储解决方案，如下图所示。

存储区域网络（Storage Area Network，SAN）是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。SAN 可以被看作是负责数据传输的后端网络，而前端网络（或称为数据网络）则负责正常的 TCP/IP 传输。也可以把 SAN 看作是通过特定互连方式连接的若干台存储服务器组成的单独的数据网络，提供企业级的数

据存储服务，其拓扑结构如下图所示。




**参考答案**

（64）D

**试题（65）**

IEEE 802.11 采用了类似于 802.3 CSMA/CD 协议的 CSMA/CA 协议，之所以不采用 CSMA/CD 协议的原因是__（65）__。

（65）A．CSMA/CA 协议的效率更高　　B．CSMA/CD 协议的开销更大

C．为了解决隐蔽终端问题　　D．为了引进其他业务

**试题（65）分析**

CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫作载波监听多路访问/冲突避免协议。在无线网中进行冲突检测有时是困难的，例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔（Inter Frame Spacing，IFS）时间。另外还有一个后退计数器，它的初始值是随机设置的，递减计数直到 0。基本的操作过程是：

① 如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后

退计数器并坚持监听。

② 听到信道空闲后等待 IFS 时间，然后开始计数。最先计数完的站可以开始发送。

③ 其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成开始发送。

分析这个算法发现，两次 IFS 之间的间隔是各个站竞争发送到时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

**参考答案**

（65）C

**试题（66）**

建筑物综合布线系统中的工作区子系统是指__（66）__。

（66）A. 由终端到信息插座之间的连线系统

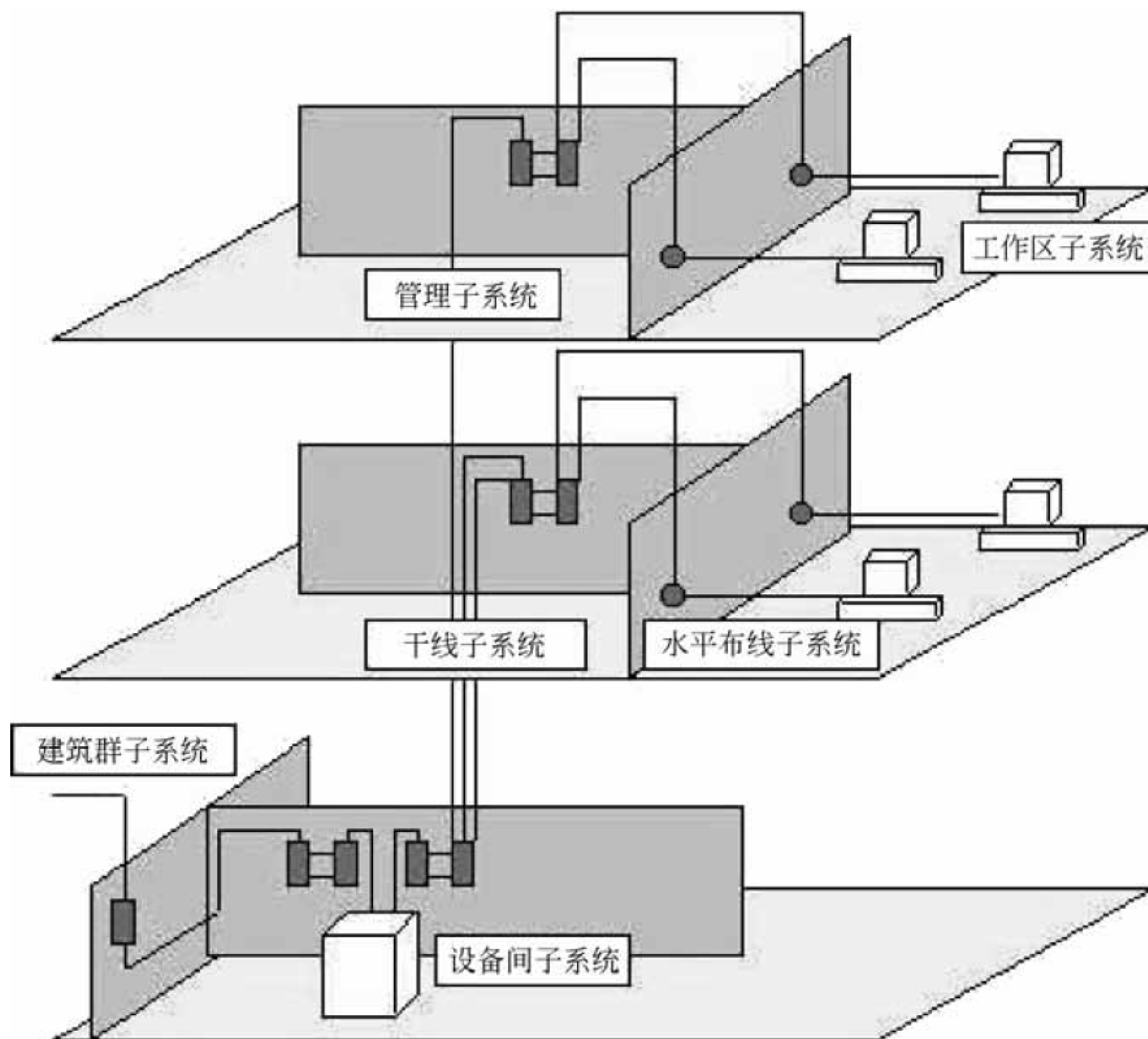
B. 楼层接线间的配线架和线缆系统

C. 各楼层设备之间的互连系统

D. 连接各个建筑物的通信系统

**试题（66）分析**

建筑物综合布线系统分为 6 个子系统：工作区子系统、水平布线子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如下图所示。



工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区，工作区应支持电话、数据终端、计算机、电视机、监视器，以及传感器等多种终端设备。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平布线子系统的作用是将干线子系统线路延伸到用户工作区。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头接于设备间的主配线架上，另一头接在楼层接线间的管理配线架上。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX，网络设备和监控设备等）之间的连接。

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。

**参考答案**

（66）A

**试题（67）**

EIA/TIA-568 标准规定，在综合布线时，如果信息插座到网卡之间使用无屏蔽双绞线，布线距离最大为＿（67）＿m。

（67）A. 10　　B. 30　　C. 50　　D. 100

**试题（67）分析**

在进行结构化布线系统设计时，要考虑线缆长度的限制，下表是 EIA/TIA-568 标准提出的布线距离最大值。

| 子　系　统 | 光纤（m） | 屏蔽双绞线（m） | 无屏蔽双绞线（m） |
|---|---|---|---|
| 建筑群（楼栋间） | 2000 | 800 | 700 |
| 主干（设备间到配线间） | 2000 | 800 | 700 |
| 配线间到工作区信息插座 |  | 90 | 90 |
| 信息插座到网卡 |  | 10 | 10 |

**参考答案**

（67）A

**试题（68）**

网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行，其中，数据库容灾属于＿（68）＿。

（68）A. 物理线路安全和网络安全 B. 应用安全和网络安全
C. 系统安全和网络安全 D. 系统安全和应用安全

**试题（68）分析**

网络安全体系设计是逻辑设计工作的重要内容之一，数据库容灾属于系统安全和应用安全考虑范畴。

**参考答案**

（68）D

**试题（69）**

下列关于网络核心层的描述中，正确的是__（69）__。

（69）A. 为了保障安全性，应该对分组进行尽可能多的处理
B. 将数据分组从一个区域高速地转发到另一个区域
C. 由多台二、三层交换机组成
D. 提供多条路径来缓解通信瓶颈

**试题（69）分析**

三层模型主要将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用。核心层提供不同区域或者下层的高速连接和最优传送路径；汇聚层将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略；接入层为局域网接入广域网或者终端用户访问网络提供接入。其中核心层是互连网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。

在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

核心层应具有有限的和一致的范围，如果核心层覆盖的范围过大，连接的设备过多，必然引起网络的复杂度加大，导致网络管理性降低；同时，如果核心层覆盖的范围不一致，必然导致大量处理不一致情况的功能都在核心层网络设备中实现，会降低核心网络设备的性能。

对于那些需要连接因特网和外部网络的网络工程来说，核心层应包括一条或多条连接到外部网络的连接，这样可以实现外部连接的可管理性和高效性。

**参考答案**

（69）B

**试题（70）**

网络系统设计过程中，物理网络设计阶段的任务是__（70）__。

（70）A. 依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境
B. 分析现有网络和新网络的各类资源分布，掌握网络所处的状态
C. 根据需求规范和通信规范，实施资源分配和安全规划
D. 理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

**试题（70）分析**

网络的生命周期至少包括网络系统的构思计划、分析设计、实时运行和维护的过程。对于大多数网络系统来说，由于应用的不断发展，这些网络系统需要进行不断重复设计、实施、维护的过程。其中：

网络逻辑结构设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并基于该逻辑结构实施后续的资源分配规划、安全规划等内容。

物理网络设计是对逻辑网络设计的物理实现，通过对设备的具体物理分布、运行环境等的确定，确保网络的物理连接符合逻辑连接的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务。

现有网络体系分析的工作目的是描述资源分布，以便于在升级时尽量保护已有投资，通过该工作可以使网络设计者掌握网络现在所处的状态和情况。

需求分析阶段有助于设计者更好地理解网络应该具有什么功能和性能，最终设计出符合用户需求的网络，它为网络设计提供依据。

**参考答案**

（70）A

**试题（71）～（75）**

Routing protocols use different techniques for assigning __（71）__ to individual networks. Further, each routing protocol forms a metric aggregation in a different way. Most routing protocols can use multiple paths if the paths have an equal __（72）__. Some routing protocols can even use multiple paths when paths have an unequal cost. In either case, load __（73）__ can improve overall allocation of network bandwidth. When multiple paths are used, there are several ways to distribute the packets. The two most common mechanisms are per-packet load balancing and per-destination load balancing. Per-packet load balancing distributes the __（74）__ across the possible routes in a manner proportional to the route metrics. Per-destination load balancing distributes packets across the possible routes based on __（75）__.

（71）A. calls　　B. metrics　　C. links　　D. destinations

（72）A. user　　B. distance　　C. entity　　D. cost

（73）A. bracketing　　B. balancing　　C. downloading　　D. transmitting

（74）A. destinations　　B. resources　　C. packets　　D. sources

（75）A. destinations　　B. resources　　C. packets　　D. Sources

**参考译文**

各种路由协议使用不同的技术来为网络赋予度量值。进一步说，每一种路由协议都形成了不同的度量汇聚模式。大部分路由协议在各个通路具有相等费用时可以使用多个通

路。某些路由协议甚至在各个通路费用不相等时也可以使用多个通路。在上述任何一种情况下，负载均衡都可以改进网络带宽的全局分配。当使用多个通路时，可以使用多种方法来分配分组。两种最通常的机制是按分组进行负载均衡和按目标进行负载均衡。按分组进行负载均衡是指按照路由度量的比例向各个可能的路由上分配分组。按目标进行负载均衡是指根据目标向各个可能的路由上分配分组。

**参考答案**

（71）B （72）D （73）B （74）C （75）A

# 第 4 章　2009 下半年网络工程师下午试题分析与解答

## 试题一（共 15 分）

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某校园网中的无线网络拓扑结构如图 1-1 所示。

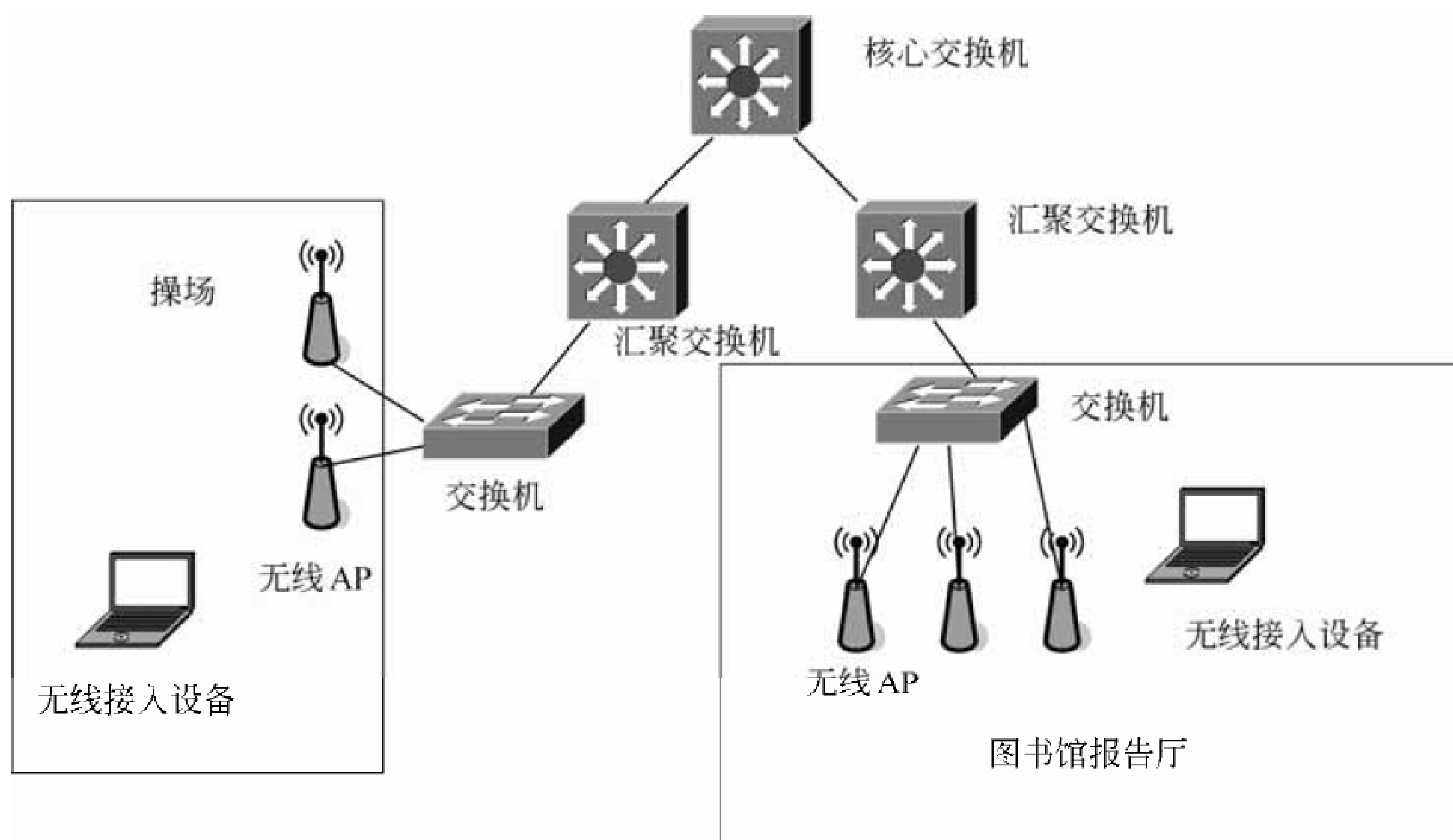



图 1-1

该网络中无线网络的部分需求如下：

1. 学校操场要求部署 AP，该操场区域不能提供外接电源。
2. 学校图书馆报告厅要求高带宽、多接入点。
3. 无线网络接入要求有必要的安全性。

【问题 1】

根据学校无线网络的需求和拓扑图可以判断，连接学校操场无线 AP 的是__（1）__交换机，它可以通过交换机的__（2）__口为 AP 提供直流电。

【问题 2】

1. 根据需求在图书馆报告厅安装无线 AP。如果采用符合 IEEE 802.11b 规范的 AP，理论上最高可以提供__（3）__Mb/s 的传输速率；如果采用符合 IEEE 802.11g 规范的 AP，理论上最高可以提供__（4）__Mb/s 的传输速率。如果采用符合__（5）__规范的 AP，

由于将 MIMO 技术和___（6）___调制技术结合在一起，理论上最高可以提供 600Mbps 的传输速率。

（5）备选答案：

A. IEEE 802.11a　　B. IEEE 802.11e

C. IEEE 802.11i　　D. IEEE 802.11n

（6）备选答案：

A. BFSK　　B. QAM　　C. OFDM　　D. MFSK

2．图书馆报告厅需要部署 10 台无线 AP，在配置过程中发现信号相互干扰严重，这时应调整无线 AP 的___（7）___设置，用户在该报告厅内应选择___（8）___，接入不同的无线 AP。

（7）、（8）备选答案：

A．频道　　B．功率　　C．加密模式　　D．操作模式

E．SSID

**【问题 3】**

若在学校内一个专项实验室配置无线 AP，为了保证只允许实验室的 PC 机接入该无线 AP，可以在该无线 AP 上设置不广播___（9）___，对客户端的___（10）___地址进行过滤，同时为保证安全性，应采用加密措施。无线网络加密主要有三种方式：___（11）___、WPA/WPA2、WPA-PSK/WPA2-PSK。在这三种模式中，安全性最好的是___（12）___，其加密过程采用了 TKIP 和___（13）___算法。

（13）备选答案：

A．AES　　B．DES　　C．IDEA　　D．RSA

**试题一分析**

本题考查无线网络的部署问题。

**【问题 1】**

本问题考查 POE 知识。根据题目要求，学校操场要求部署 AP，该操场区域不能提供外接电源，所以应采用 POE 技术供电。

POE（Power Over Ethernet）指的是在现有的以太网 Cat.5 布线基础架构不做任何改动的情况下，在为一些基于 IP 的终端（如 IP 电话机、无线局域网接入点 AP、网络摄像机等）传输数据信号的同时，还能为此类设备提供直流供电的技术。POE 技术能在确保现有结构化布线安全的同时现有网络的正常运作，最大限度地降低成本。

POE 也被称为基于局域网的供电系统（Power over LAN，POL）或有源以太网（Active Ethernet），有时也被简称为以太网供电，这是利用现存标准以太网传输电缆的同时传送数据和电功率的最新标准规范，并保持了与现存以太网系统和用户的兼容性。IEEE 802.3af 标准是基于以太网供电系统 POE 的新标准，它在 IEEE 802.3 的基础上增加了通过网线直接供电的相关标准，是现有以太网标准的扩展，也是第一个关于电源分配的国际标准。

**【问题 2】**

本问题考查 802.11 的标准规范问题。

802.11 是 IEEE 最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到 2Mbps。由于它在速率和传输距离上都不能满足人们的需要，因此 IEEE 小组又相继推出了多个新标准，主要如下：

IEEE 802.11a（Wi-Fi5）标准是得到广泛应用的 802.11b 标准的后续标准，工作在 5GHzU-NII 频带，物理层速率可达 54Mbps，传输层可达 25Mbps；可提供 25Mbps 的无线 ATM 接口和 10Mbps 的以太网无线帧结构接口，以及 TDD/TDMA 的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

IEEE802.11b 是无线局域网的一个标准。其载波的频率为 2.4GHz，传送速度为 11Mbit/s。IEEE 802.11b 在 2.4-GHz-ISM 频段共有 14 个频宽为 22MHz 的频道可供使用。IEEE 802.11b 的后继标准是 IEEE 802.11g，其传送速度为 54Mb/s。

IEEE 802.11n 是 2004 年 1 月 IEEE 宣布组成的一个新的单位来发展新的 802.11 标准，它增加了 MIMO（multiple-input multiple-output）的标准。利用 MIMO 使用多个发射和接收天线来允许更高的资料传输率。IEEE 802.11n 将 MIMO 技术与 OFDM 调制技术结合在一起，理论上最高可以提供 600Mbps 的传输速率。

无线 AP 一般在某个频段工作。当在某个区域有多个无线 AP，且使用同一频道时，可能出现信号相互干扰严重的问题。在某个频段下，实际有多个频道，可以通过手动方式修改无线 AP 所使用的频道，或在无线 AP 上安装一个 5GHz 的组件。5GHz 可以使用的频段有 23 个，且几乎没有其他人在使用，这样可以解决信号相互干扰的问题。另外，在无线 AP 中，SSID（Service Set Identifier）用来区分不同的网络，最多可以有 32 个字符，无线网卡设置不同的 SSID 就可以进入不同网络，SSID 通常由AP广播出来，用户选择不同的 SSID，接入不同的无线 AP。

**【问题 3】**

本问题考查配置无线 AP 安全的问题。

解决无线 AP 安全，首先要通过 SSID 和 MAC 地址过滤防止非法链接。

SSID 用来区分无线访问节点所使用的初始化字符串，客户端要通过 SSID 来完成链接的初始化。该校验器由制造商进行设定，同一厂商产品使用同样的默认值。如果使用厂家的初始化字符串，那么就可能被非授权链接。因此，在配置无线网络时，应更改 SSID 初始化字符串，使其难于猜测，并在条件许可的情况下限制 SSID 广播，以此来杜绝非法链接。

在无线 AP 中，可以设置 MAC 地址过滤，这样只用指定的 MAC 地址才能登录无线 AP，从而保证杜绝非法链接。

为保证无线网络的安全性，还应采用加密措施。无线网络加密主要有三种方式：

WEP、WPA/WPA2 和 WPA-PSK/WPA2-PSK。

无线网络最初采用的安全机制是 WEP（有线等效私密），但是后来发现 WEP 是很不安全的，802.11 组织开始着手制定新的安全标准，也就是后来的 802.11i 协议。但是标准的制定到最后的发布需要较长的时间，而且考虑到消费者不会为了网络的安全性而放弃原来的无线设备，因此 Wi-Fi 联盟在标准推出之前，在 802.11i 草案的基础上制定了一种称为 WPA（Wi-Fi Protected Access）的安全机制，它使用 TKIP（临时密钥完整性协议），使用的加密算法还是 WEP 中使用的加密算法 RC4，所以不需要修改原来无线设备的硬件，WPA 针对 WEP 中存在的问题：IV 过短、密钥管理过于简单、对消息完整性没有有效的保护，通过软件升级的方法提高了网络的安全性。

在 802.11i 颁布之后，Wi-Fi 联盟推出了 WPA-PSK/WPA2-PSK，它支持 AES（高级加密算法），因此需要新的硬件支持，使用 CCMP（计数器模式密码块链消息完整码协议），其安全性最好。

**参考答案**

**【问题 1】**

（1）PoE （或答 802.3af 也给全分）

（2）以太（或 Ethernet）

**【问题 2】**

（3）11

（4）54

（5）D

（6）C

（7）A

（8）E

**【问题 3】**

（9）SSID

（10）MAC（或物理地址）

（11）WEP（或有线等效加密）

（12）WPA-PSK/WPA2-PSK 或 WPA/WPA2

（13）A

**试题二（共 15 分）**

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

网络拓扑结构如图 2-1 所示。

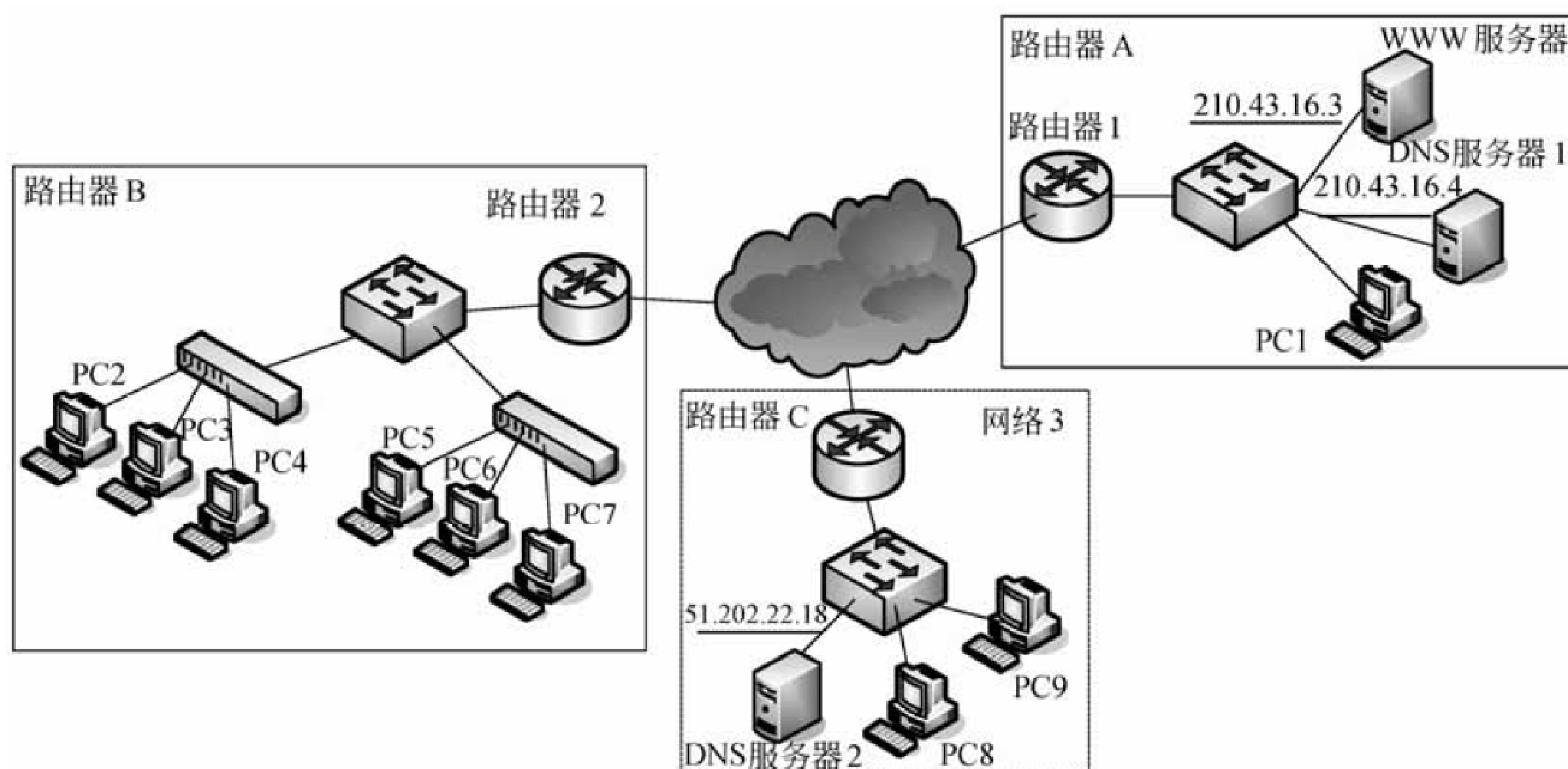



图 2-1

【问题 1】

网络 A 的 WWW 服务器上建立了一个 Web 站点，对应的域名是 www.abc.edu。DNS 服务器 1 上安装 Windows Server 2003 操作系统并启用 DNS 服务。为了解析 WWW 服务器的域名，在图 2-2 所示的对话框中，新建一个区域的名称是__（1）__；在图 2-3 所示的对话框中，添加的对应的主机“名称”为__（2）__。

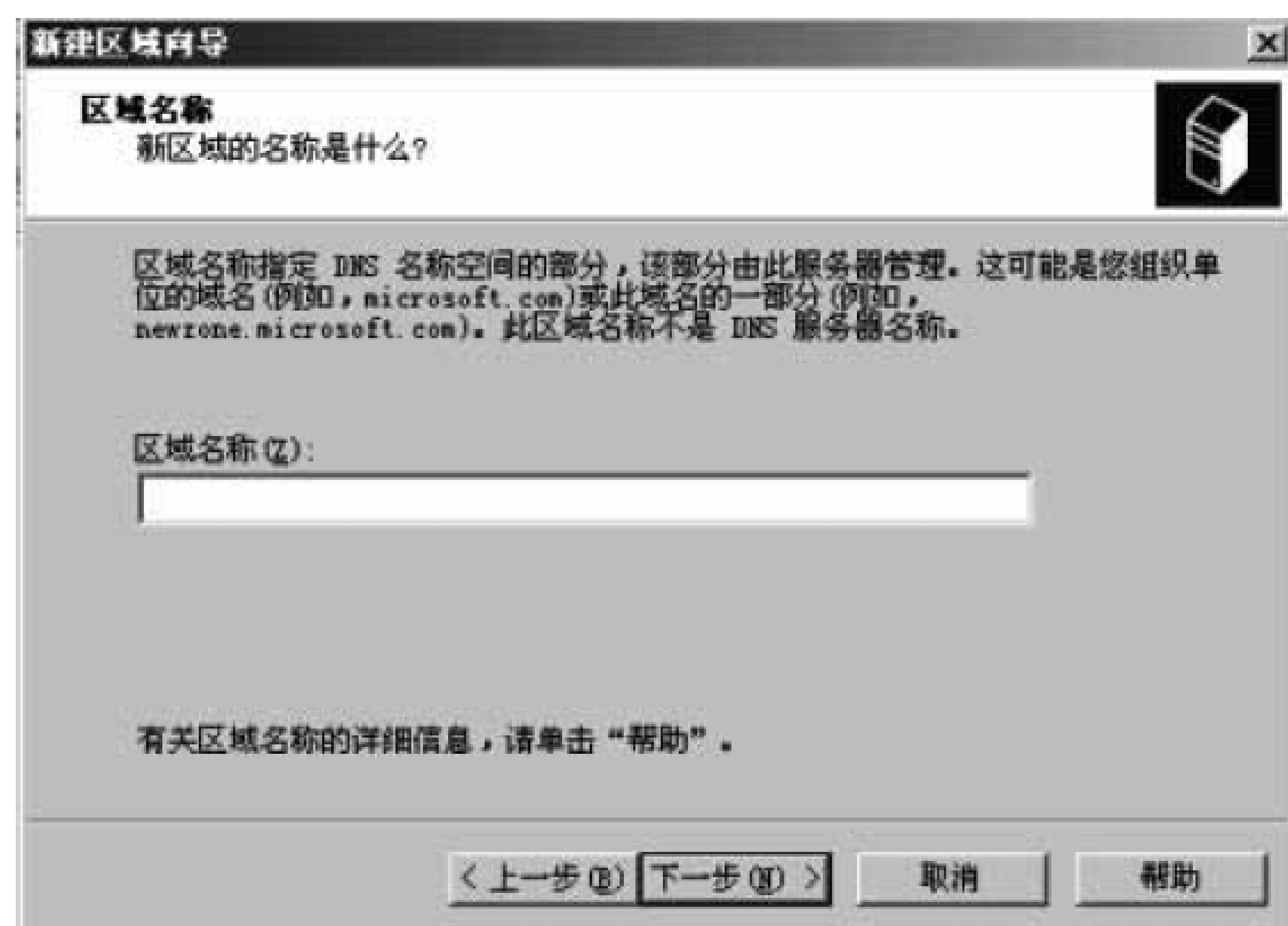



图 2-2

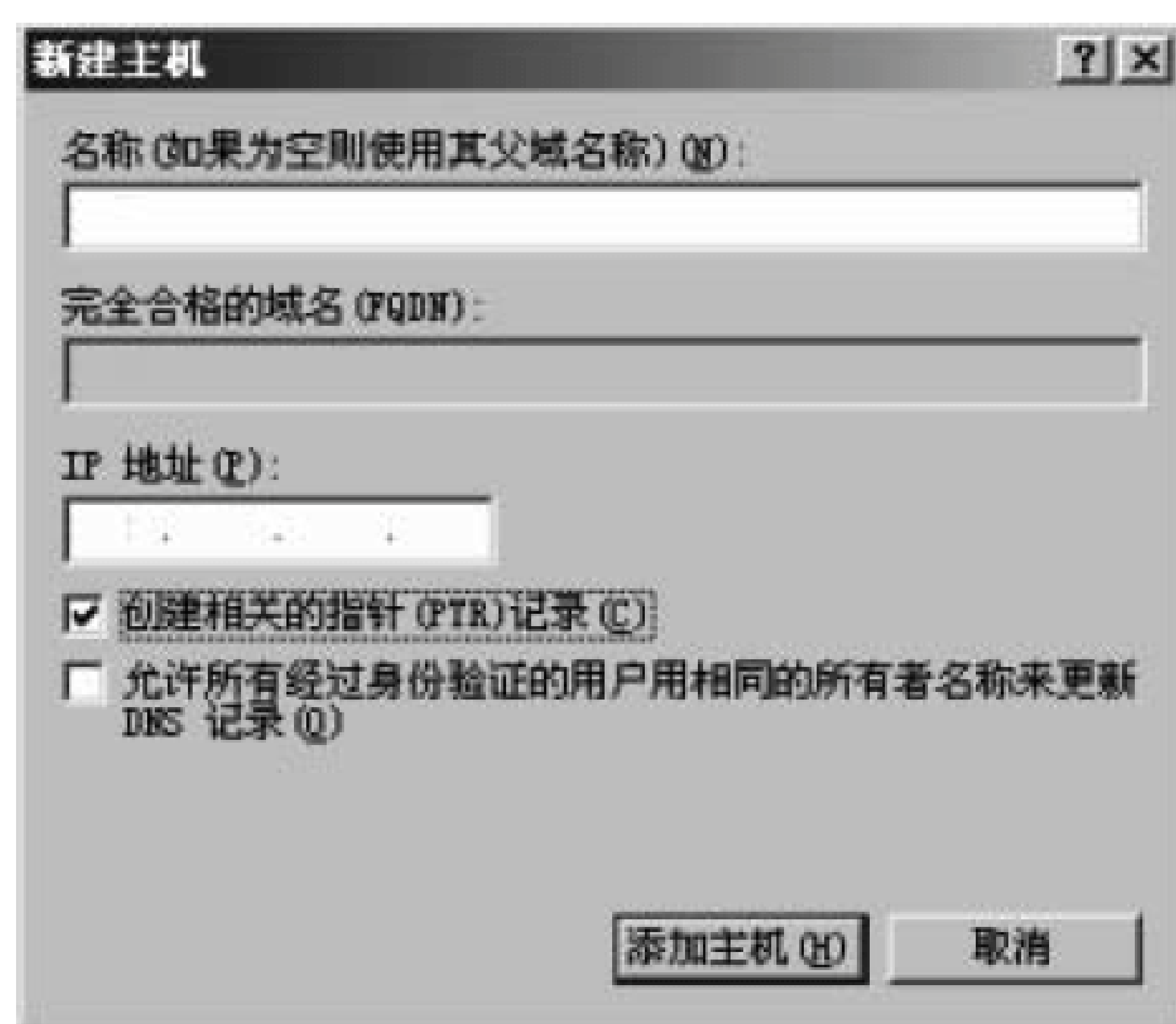



图 2-3

【问题 2】

在 DNS 系统中反向查询（Reverse Query）的功能是__（3）__。为了实现网络 A 中 WWW 服务器的反向查询，在图 2-4 和图 2-5 中进行配置，其中网络 ID 应填写为__（4）__，主机名应填写为__（5）__。

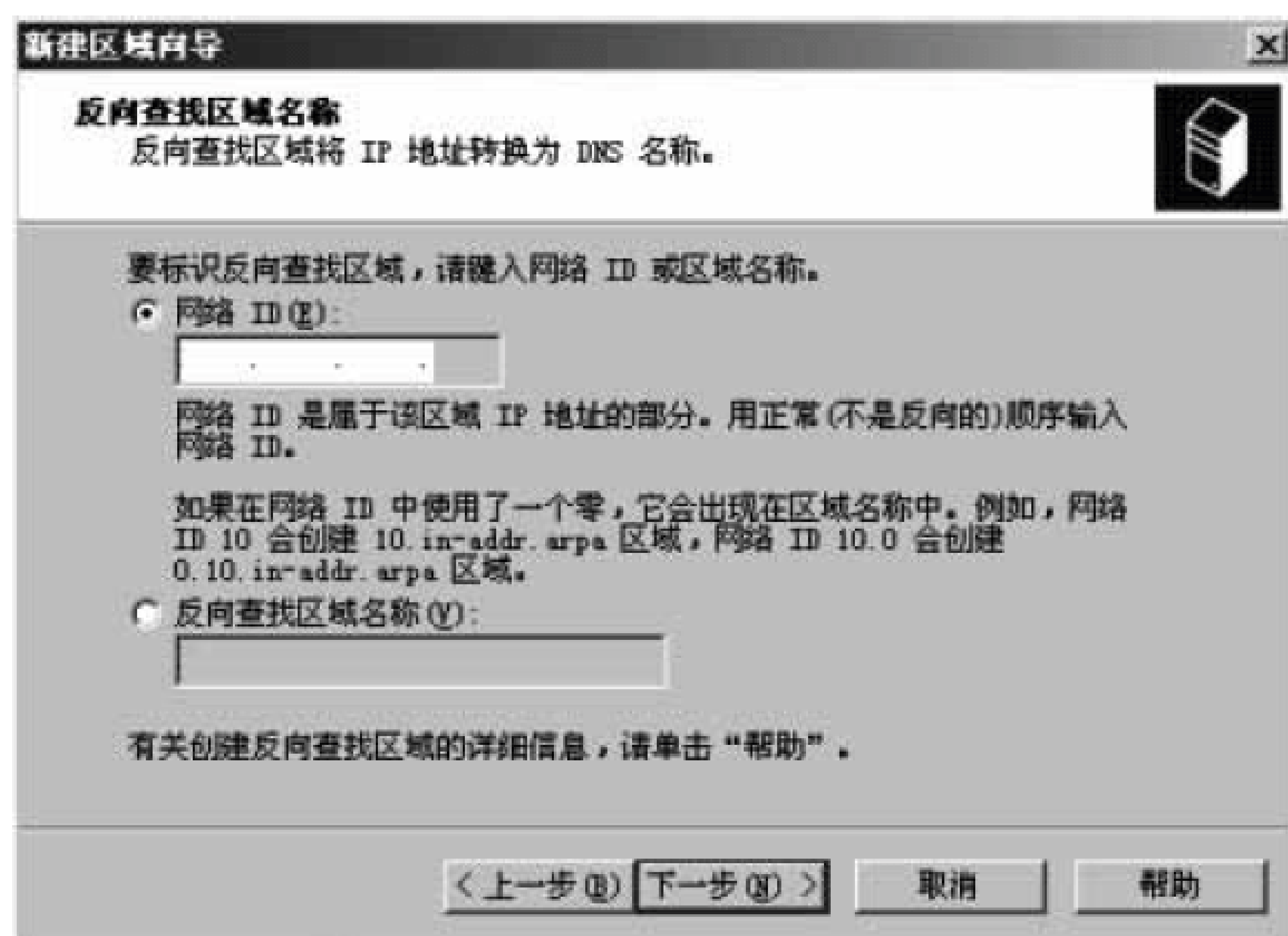



图 2-4

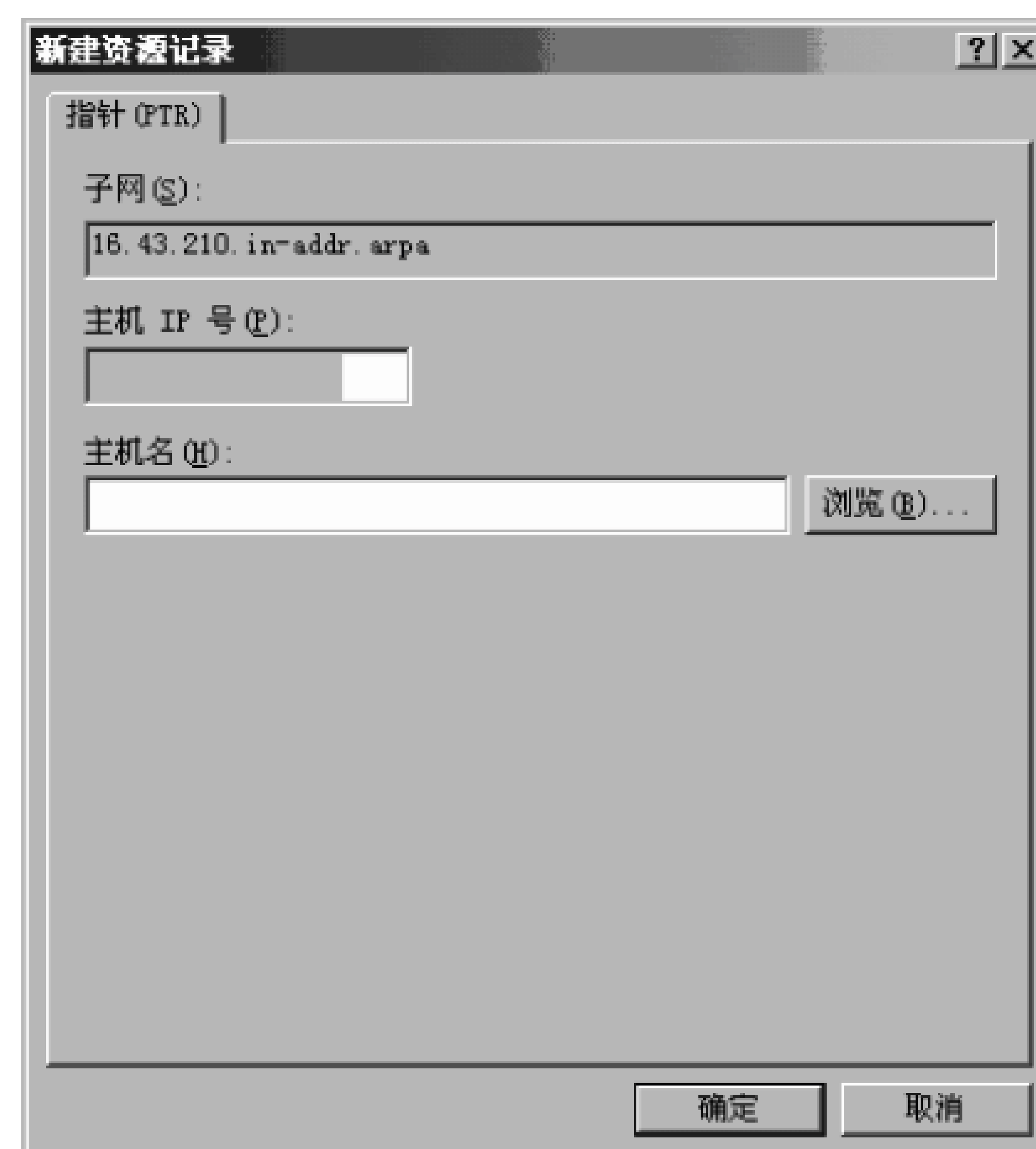



图 2-5

【问题 3】

DNS 服务器 1 负责本网络区域的域名解析，对于非本网络的域名，可以通过设置"转发器"，将自己无法解析的名称转到网络 C 中的 DNS 服务器 2 进行解析。设置步骤：首先在"DNS 管理器"中选中 DNS 服务器，单击鼠标右键，选择"属性"对话框中的"转发器"选项卡，在弹出的如图 2-6 所示的对话框中应如何配置？

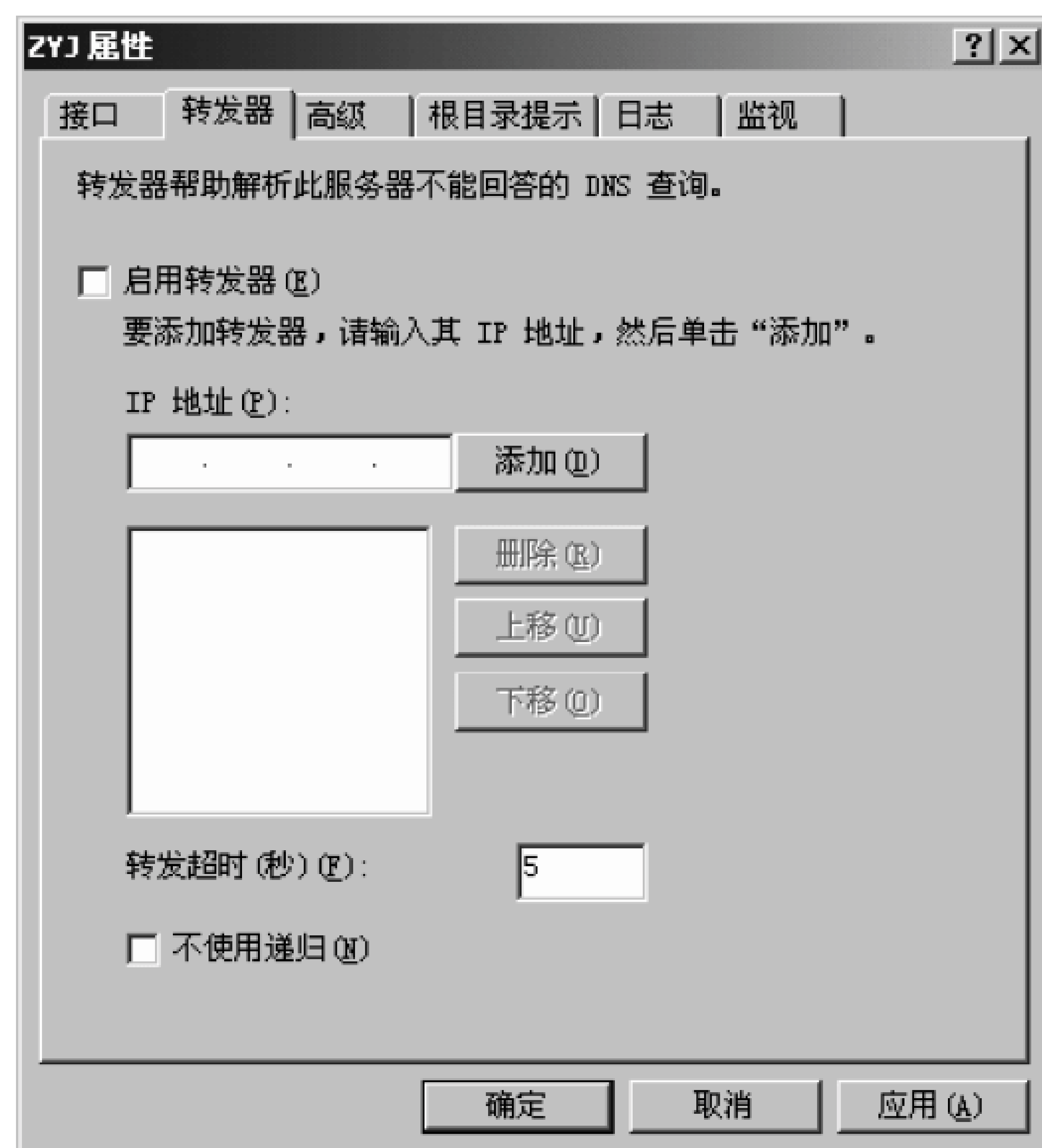



图 2-6

【问题 4】

网络 C 的 Windows Server 2003 服务器上配置了 DNS 服务，在该服务器上两次使用

nslookup www.sohu.com 命令得到的结果如图 2-7 所示，由结果可知，该 DNS 服务器（6）。

（6）备选答案：

A. 启用了循环功能　　B. 停用了循环功能

C. 停用了递归功能　　D. 启用了递归功能

```
C:\Documents and Settings\Administrator>nslookup www.sohu.com
Server:  ns.test.com
Address:  51.202.22.18
Non-authoritative answer:
Name:    pgcrtbjt01.a.sohu.com
Addresses:  222.35.250.137, 222.35.250.138, 222.35.250.139, 222.35.250.132
        22235.250.133, 222.35.250.134, 222.35.250.135, 222.35.250.136
Aliases:  www.sohu.com, d7.a.sohu.com

C:\Documents and Settings\Administrator>nslookup www.sohu.com
Server:  ns.test.com
Address:  51.202.22.18
Non-authoritative answer:
Name:    pgcrtbjt01.a.sohu.com
Addresses:  222.35.250.135, 222.35.250.136, 222.35.250.137, 222.35.250.138
        22235.250.139, 222.35.250.132, 222.35.250.133, 222.35.250.134
Aliases:  www.sohu.com, d7.a.sohu.com
```

图 2-7

**【问题 5】**

在网络 B 中，除 PC5 计算机以外，其他的计算机都能访问网络 A 的 WWW 服务器，而 PC5 计算机与网络 B 内部的其他 PC 都是连通的。分别在 PC5 和 PC6 上执行命令 ipconfig，结果信息如 2-8 图（a）和 2-8（b）所示：

```
Ethernet   adapter  本地连接:
   Connection－specific DNS Suffix  .   :
        IP Address . . . . . . . . . . . . . :  192.168.0.100
        Subnet Mask. . . . . . . . . . . . :  255.255.255.0
        Default    Gateway . . . . . . . . :  192.168.1.3
```

（a）

```
Ethernet   adapter  本地连接:
   Connection－specific DNS Suffix  .   :
        IP Address . . . . . . . . . . . . . :  192.168.0.247
        Subnet Mask. . . . . . . . . . . . :  255.255.255.0
        Default    Gateway . . . . . . . . :  192.168.0.3
```

（b）

图 2-8

请问 PC5 的故障原因是什么？如何解决？

**试题二分析**

本题考查 Windows Server 2003 操作系统中 DNS 服务器的配置。

**【问题 1】**

由网络 A 的 WWW 服务器对应的域名是 www.abc.edu，故在 DNS 服务器上新建的区域的名称是 abc.edu，主机名称为 www。

**【问题 2】**

在 DNS 系统中可利用反向查询功能来依据 IP 地址查询对应的域名。Windows Server 2003 操作系统中配置 DNS 反向查询时 IP 地址倒写，且只取前 3 个字节，故（4）应填入"210.43.16"，对应的主机名为www.abc.edu。

**【问题 3】**

转发器的功能是将自己无法解析的名称转到另一个 DNS 服务器进行转发，配置转发服务器时需要指定转发服务器的 IP 地址。故在图中应选中"启用转发器"复选框，并在 IP 地址栏输入 DNS 服务器 2 的 IP 地址，即"51.202.22.18"。

**【问题 4】**

从 DNS 服务器上两次使用 nslookup 得到的结果可以看出，该 DNS 服务器启用了循环功能。

**【问题 5】**

PC5 和 PC6Internet 协议属性参数中网关地址不同，故 PC5 的默认网关配置错误。将其默认网关 IP 地址修改为"192.168.0.3"即可。

**参考答案**

**【问题 1】**

（1）abc.edu

（2）www

**【问题 2】**

（3）用 IP 地址查询对应的域名

（4）210.43.16

（5）www.abc.edu

**【问题 3】**

选中"启用转发器"复选框，在 IP 地址栏输入"51.202.22.18"，单击"添加"按钮，然后单击"确定"按钮关闭对话框。

**【问题 4】**

（6）A

**【问题 5】**

PC5 的默认网关配置错误。

将默认网关 IP 地址修改为“192.168.0.3”。

**试题三（共 15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

在大型网络中，通常采用 DHCP 完成基本网络配置会更有效率。

**【问题 1】**

在 Linux 系统中，DHCP 服务默认的配置文件为__（1）__。

（1）备选答案：

A．/etc/dhcpd.conf　　B．/etc/dhcpd.config

C．/etc/dhcp.conf　　D．/etc/dhcp.config

**【问题 2】**

管理员可以在命令行通过__（2）__命令启动 DHCP 服务；通过__（3）__命令停止 DHCP 服务。

（2）、（3）备选答案：

A．service dhcpd start　　B．service dhcpd up

C．service dhcpd stop　　D．service dhcpd down

**【问题 3】**

在 Linux 系统中配置 DHCP 服务器，该服务器配置文件的部分内容如下：

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   option routers           192.168.1.254;
   option subnet-mask       255.255.255.0;
   option broadcast-address        192.168.1.255;
   option domain-name-servers      192.168.1.3;
   range 192.168.1.100  192.168.1.200;
   default-lease-time 21600;
   max-lease-time 43200;
       host webserver {
         hardware ethernet 52:54:AB:34:5B:09;
         fixed-address 192.168.1.100;
    }
}
```

在主机 webserver 上运行 ifconfig 命令时显示如下，根据 DHCP 配置，填写空格中缺少的内容。

```
eth0      Link encap:Ethernet   HWaddr  （4）
           inet addr: （5）   Bcast:192.168.1.255   Mask: （6）
           UP BROADCAST RUNNING MULTICAST   MTU:1500   Metric:1
           RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:100
           RX bytes:0 (0.0 b)   TX bytes:168 (168.0 b)
           Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
           inet addr:127.0.0.1   Mask:255.0.0.0
           UP LOOPBACK RUNNING   MTU:16436   Metric:1
           RX packets:397 errors:0 dropped:0 overruns:0 frame:0
           TX packets:397 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:26682 (26.0 Kb)   TX bytes:26682 (26.0 Kb)
```

该网段的网关 IP 地址为 （7） ，域名服务器 IP 地址为 （8） 。

**试题三分析**

本题考查 Linux 下的 DHCP 服务配置相关问题。

**【问题 1】**

在 Linux 系统中，DHCP 服务默认的配置文件为/etc/dhcpd.conf。

**【问题 2】**

在 Linux 系统中，可以在命令行下通过 service dhcpd start 和 service dhcpd stop 进行 DHCP 服务的启动和停止。

**【问题 3】**

问题（4）～（6）是 webserver 的 MAC 地址、IP 地址和网络掩码。在/etc/dhcpd.conf 中有如下相关内容：

```
option subnet-mask      255.255.255.0;
host webserver {
        hardware ethernet 52:54:AB:34:5B:09;
        fixed-address 192.168.1.100;
   }
```

因此可以知道 webserver 的 MAC 地址是 52:54:AB:34:5B:09，IP 地址是 192.168.1.100，网路掩码为 255.255.255.0。

从 dhcpd.conf 中可以看到如下内容：

```
option routers          192.168.1.254;
 option domain-name-servers      192.168.1.3;
```

因此该网段的网关 IP 地址为 192.168.1.254，DNS 为 192.168.1.3。

**参考答案**

**【问题 1】**

（1）A

**【问题 2】**

（2）A

（3）C

**【问题 3】**

（4）52:54:AB:34:5B:09

（5）192.168.1.100

（6）255.255.255.0

（7）192.168.1.254

（8）192.168.1.3

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司通过 PIX 防火墙接入 Internet，网络拓扑如图 4-1 所示。

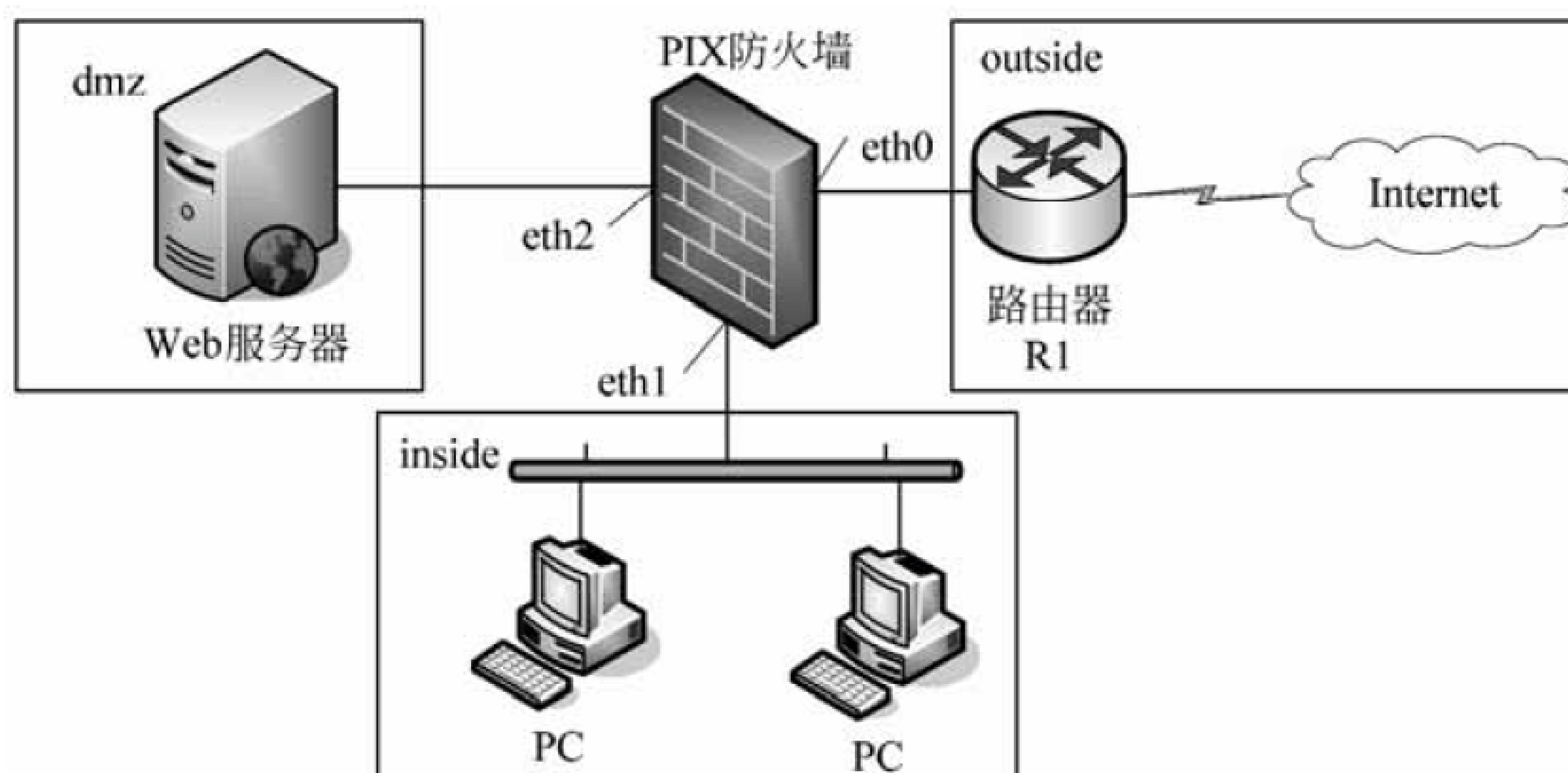



图 4-1

在防火墙上利用 show 命令查询当前配置信息如下：

```
PIX#show config
...
nameif eth0 outside security0
nameif eth1 inside security100
nameif eth2 dmz security40
...
```

```
fixup protocol ftp 21                                  (1)
fixup protocol http 80
...
ip address outside 61.144.51.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
ip address dmz 10.10.0.1 255.255.255.0
...
global (outside) 1 61.144.51.46
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
...
route outside 0.0.0.0 0.0.0.0 61.144.51.45 1          (2)
...
```

**【问题 1】**

解释（1)、(2）处画线语句的含义。

**【问题 2】**

根据配置信息，填写表 4-1。

**表 4-1**

| 域　名　称 | 接 口 名 称 | IP 地址 | IP 地址掩码 |
|---|---|---|---|
| inside | eth1 | （3） | 255.255.255.0 |
| outside | eth0 | 61.144.51.42 | （4） |
| dmz | （5） | （6） | 255.255.255.0 |

**【问题 3】**

根据所显示的配置信息，由 inside 域发往 Internet 的 IP 分组，在到达路由器 R1 时的源 IP 地址是＿（7）＿。

**【问题 4】**

如果需要在 dmz 域的服务器（IP 地址为 10.10.0.100）对 Internet 用户提供 Web 服务（对外公开 IP 地址为 61.144.51.43)，请补充完成下列配置命令。

PIX(config)#static (dmz, outside) ＿（8）＿ ＿（9）＿

PIX(config)#conduit permit tcp host ＿（10）＿ eq www any

**试题四分析**

本题考查 PIX 防火墙的配置。

**【问题 1】～【问题 3】**

使用 show config 命令得到的配置信息解释如下：

```
nameif eth0 outside security0  //eth0 接口的名称为 outside，安全级别为 0
```

```
nameif eth1 inside security100 //eth1 接口的名称为 inside，安全级别为 100
nameif eth2 dmz security40     //eth2 接口的名称为 dmz，安全级别为 40
...
fixup protocol ftp 21           //启用 ftp 协议并使用 21 端口
fixup protocol http 80          //启用 http 协议并使用 80 端口
...
ip address outside 61.144.51.42 255.255.255.248
            //outside 接口的 IP 为 61.144.51.42，子网掩码为 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
            //inside 接口的 IP 为 192.168.0.1，子网掩码为 255.255.255.0
ip address dmz 10.10.0.1 255.255.255.0
            //dmz 接口的 IP 为 10.10.0.1，子网掩码为 255.255.255.0
...
global (outside) 1 61.144.51.46
            //发往 outside 的数据包 IP 为 61.144.51.46
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
            //inside 所有 IP 都可以访问 outside
...
route outside 0.0.0.0 0.0.0.0 61.144.51.45 1
            //outside 默认路由指向 61.144.51.45
```

**【问题 4】**

static 命令的语法如下：

```
static(internal_if_name,external_if_name)outside_ip_addr inside_ip_
address
```

根据 static 命令的语法，空（8）应该填对 outside 公开的 IP 地址 61.144.51.43，空（9）应该填 dmz 域服务器的 IP 地址 10.10.0.100。

conduit 命令用来设置允许数据从低安全级别的接口流向具有较高安全级别的接口。conduit 命令的语法如下：

```
conduit permit|deny protocol global_ip port[-port] foreign_ip [netmask]
```

根据 conduit 命令的语法，空（10）应该填 Web 服务对外公开的 IP 地址 61.144.51.43。

**参考答案**

**【问题 1】**

（1）启用 ftp 服务

（2）设置 eth0 口的默认路由，指向 61.144.51.45，且跳步数为 1

**【问题 2】**

（3）192.168.0.1

（4）255.255.255.248

（5）eth2

（6）10.10.0.1

**【问题 3】**

（7）61.144.51.46

**【问题 4】**

（8）61.144.51.43

（9）10.10.0.100

（10）61.144.51.43

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位网络拓扑结构如图 5-1 所示，要求配置 IPSec VPN 使 10.10.20.1/24 网段能够连通 10.10.10.2/24 网段，但 10.10.30.1/24 网段不能连通 10.10.10.2/24 网段。

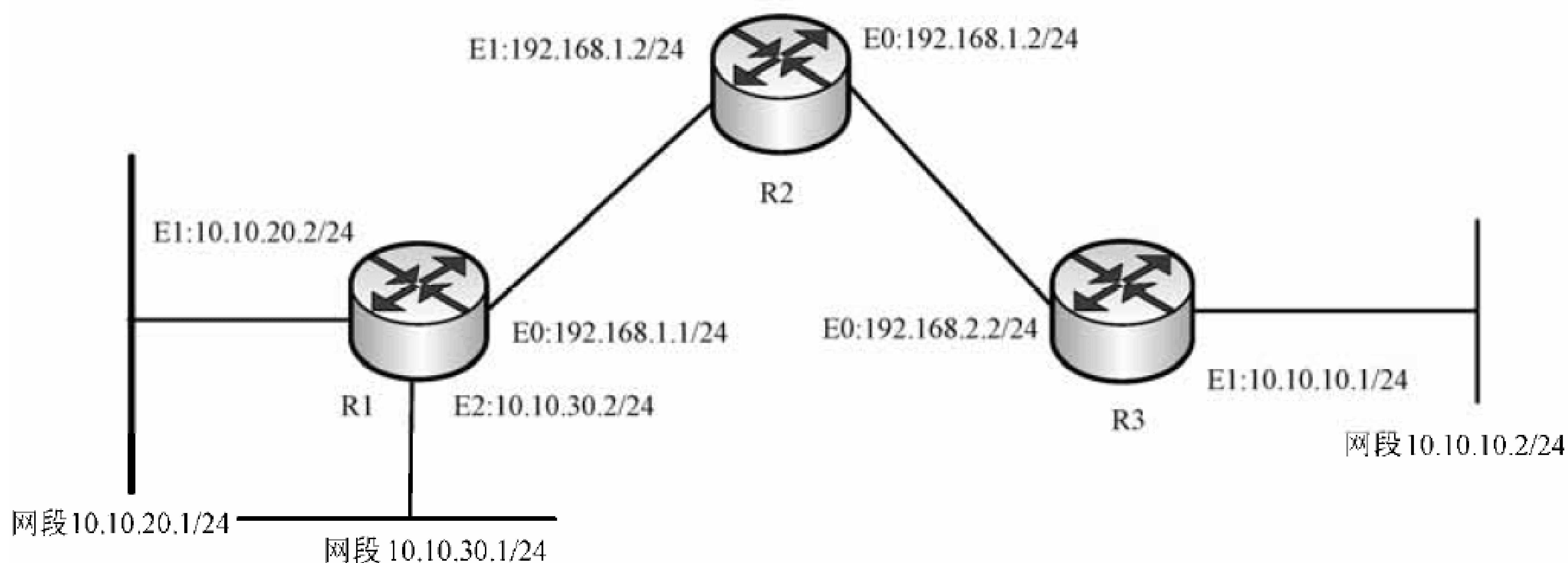



图 5-1

**【问题 1】**

根据网络拓扑和要求，解释并完成路由器 R1 上的部分配置。

R1 (config)#crypto isakmp enable　　　　（启用 IKE）

R1 (config)#crypto isakmp ＿（1）＿ 20　　　　（配置 IKE 策略 20）

**<u>R1 (config-isakmp)#authentication pre-share</u>**　　　　＿（2）＿

R1 (config-isakmp)#exit

R1 (config)#crypto isakmp key 378 address 192.168.2.2　　（配置预共享密钥为 378）

R1 (config)#access-list 101 permit ip ＿（3）＿ 0.0.0.255 ＿（4）＿ 0.0.0.255（设置 ACL）

...

**【问题 2】**

根据网络拓扑和要求，完成路由器 R2 上的静态路由配置。

```
R2 (config)#ip route ___(5)___ 255.255.255.0 192.168.1.1
R2 (config)#ip route 10.10.30.0 255.255.255.0 ___(6)___
R2 (config)#ip route 10.10.10.0 255.255.255.0 192.168.2.2
```

**【问题 3】**

根据网络拓扑和 R1 的配置，解释并完成路由器 R3 的部分配置。

```
...
R3 (config)#crypto isakmp key ___(7)___ address ___(8)___
R3 (config)# crypto transform-set testvpn ah-md5-hmac esp-des esp-md5-hmac
___(9)___
R3 (cfg-crypto-trans)#exit
R3 (config)#crypto map test 20 ipsec-isakmp
R3 (config-crypto-map)#set peer 192.168.1.1
R3 (config-crypto-map)#set transform-set___(10)___
...
```

**试题五分析**

本题考查 IPSec VPN 的配置问题。

**【问题 1】**

```
R1 (config)#crypto isakmp enable                (启用 IKE)
R1 (config)#crypto isakmp Policy 20             (配置 IKE 策略 20)
R1 (config-isakmp)#authentication pre-share (在 IKE 协商过程中使用预共享密钥认证)
R1 (config-isakmp)#exit
R1 (config)#crypto isakmp key 378 address 192.168.2.2  (配置预共享密钥为 378)
R1 (config)#access-list 101 permit ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255
(设置 ACL 允许 10.10.20.1/24 网段能够连通 10.10.10.2/24 网段)
```

**【问题 2】**

```
R2 (config)#ip route 10.10.20.0 255.255.255.0 192.168.1.1
(设置静态路由 10.10.20.0/24 下一跳地址为 192.168.1.1)
R2 (config)#ip route 10.10.30.0 255.255.255.0 192.168.1.1
(设置静态路由 10.10.30.0/24 下一跳地址为 192.168.1.1)
R2 (config)#ip route 10.10.10.0 255.255.255.0 192.168.2.2
(设置静态路由 10.10.10.0/24 下一跳地址为 192.168.2.2)
```

【问题 3】

根据 R1 配置和拓扑结构可知，R3 路由器配置 IPSec VPN 对端连接地址 192.168.1.1，其预共享密钥为 378。

```
...
R3 (config)#crypto isakmp key 378  address 192.168.1.1  （配置预共享密钥为378）
R3 (config)# crypto transform-set testvpn ah-md5-hmac esp-des esp-md5-hmac
（设置名为 testvpn 的 VPN，采用 MD5 认证、DES 进行数据加密）
R3 (cfg-crypto-trans)#exit
R3 (config)#crypto map test 20 ipsec-isakmp
（crypto map 名为 test，优先级 20，IPSec 链接采用 IKE 自动协商）
R3 (config-crypto-map)#set peer 192.168.1.1
(指定此 VPN 链路，对端的 IP 地址为 192.168.1.1)。
R3 (config-crypto-map)#set transform-set testvpn （IPSec 传输模式的名字为testvpn）
...
```

### 参考答案

【问题 1】

（1）Policy

（2）在 IKE 协商过程中使用预共享密钥认证方式

（3）10.10.20.0

（4）10.10.10.0

【问题 2】

（5）10.10.20.0

（6）192.168.1.1

【问题 3】

（7）378

（8）192.168.1.1

（9）设置名为 testvpn 的 VPN，采用 MD5 认证、DES 进行数据加密

（10）testvpn

# 第 5 章　2010 上半年网络工程师上午试题分析与解答

**试题（1）**

计算机指令一般包括操作码和地址码两部分，为分析执行一条指令，其<u>（1）</u>。

（1）A．操作码应存入指令寄存器（IR），地址码应存入程序计数器（PC）

B．操作码应存入程序计数器（PC），地址码应存入指令寄存器（IR）

C．操作码和地址码都应存入指令寄存器（IR）

D．操作码和地址码都应存入程序计数器（PC）

**试题（1）分析**

本题考查指令系统基础知识。

程序被加载到内存后开始运行，当 CPU 执行一条指令时，先把它从内存储器取到缓冲寄存器 DR 中，再送入 IR 暂存，指令译码器根据 IR 的内容产生各种微操作指令，控制其他的组成部件工作，完成所需的功能。

程序计数器（PC）具有寄存信息和计数两种功能，又称为指令计数器。程序的执行分两种情况，一是顺序执行，二是转移执行。在程序开始执行前，将程序的起始地址送入 PC，该地址在程序加载到内存时确定，因此 PC 的内容即是程序第一条指令的地址。执行指令时，CPU 将自动修改 PC 的内容，以便使其保持的总是将要执行的下一条指令的地址。由于大多数指令都是按顺序来执行的，所以修改的过程通常只是简单的对 PC 加 1。当遇到转移指令时，后继指令的地址根据当前指令的地址加上一个向前或向后转移的位移量得到，或者根据转移指令给出的直接转移地址得到。

**参考答案**

（1）C

**试题（2）、（3）**

进度安排的常用图形描述方法有 Gantt 图和 PERT 图。Gantt 图不能清晰地描述<u>（2）</u>；PERT 图可以给出哪些任务完成后才能开始另一些任务。下图所示的 PERT 图中，事件 6 的最晚开始时刻是<u>（3）</u>。

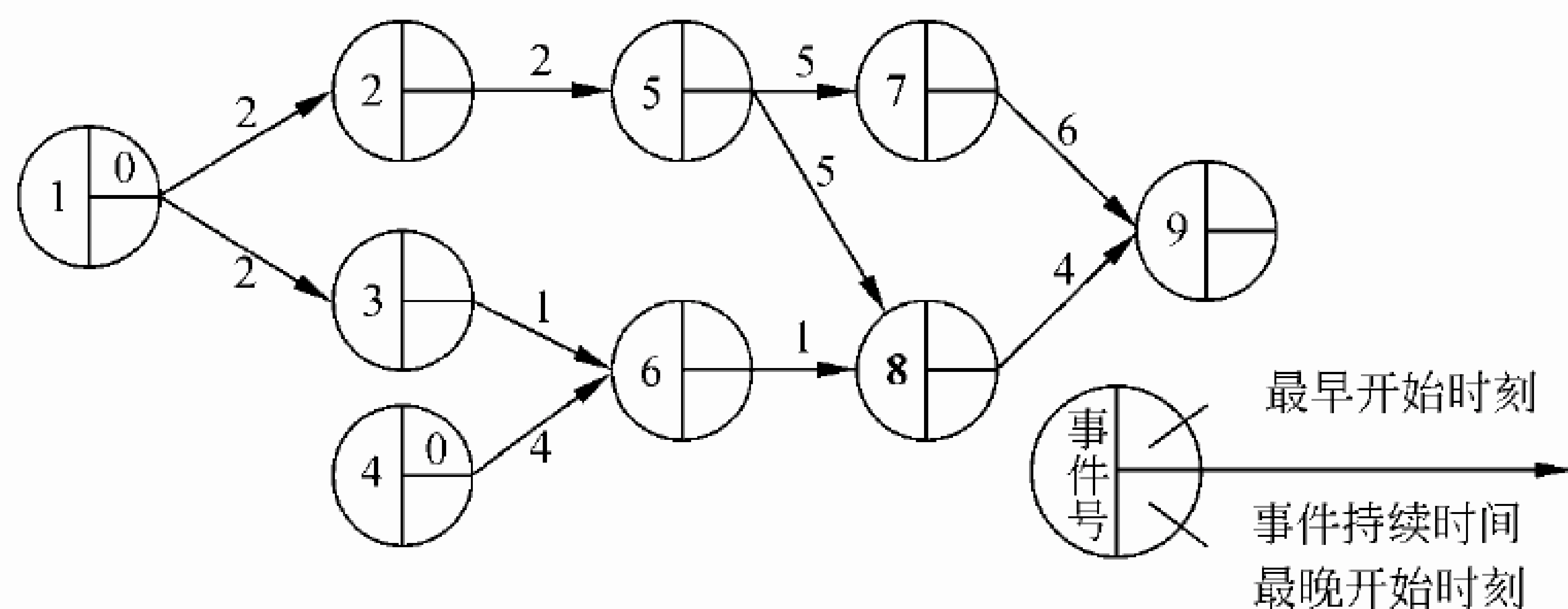
（2）A．每个任务从何时开始　　B．每个任务到何时结束

C．每个任务的进展情况　　D．各任务之间的依赖关系

（3）A．0　　B．3　　C．10　　D．11

**试题（2）、（3）分析**

本题考查软件项目计划知识。




软件项目计划的一个重要内容是安排进度，常用的方法有 Gantt 图和 PERT 图。Gantt 图用水平条状图描述，它以日历为基准描述项目任务，可以清楚地表示任务的持续时间和任务之间的并行，但是不能清晰地描述各个任务之间的依赖关系。PERT 图是一种网络模型，描述一个项目任务之间的关系。可以明确表达任务之间的依赖关系，即哪些任务完成后才能开始另一些任务，以及如期完成整个工程的关键路径。

图中任务流 1→2→5→7→9 的持续时间是 15，1→2→5→8→9 的持续时间是 13，1→3→6→8→9 的持续时间是 8，4→6→8→9 的持续时间为 9。所以项目关键路径长度为 15。事件 6 在非关键路径上，其后的任务需要时间为 5，所以最晚开始时间=15–5=10。

**参考答案**

（2）D （3）C

**试题（4）**

使用白盒测试方法时，应根据__（4）__和指定的覆盖标准确定测试数据。

（4）A．程序的内部逻辑 B．程序结构的复杂性

C．使用说明书 D．程序的功能

**试题（4）分析**

本题考查软件测试方法中白盒测试的基础知识。

白盒测试也称为结构测试，根据程序的内部结构和逻辑来设计测试用例，对程序的执行路径和过程进行测试，检查是否满足设计的需要。白盒测试常用的技术涉及不同覆盖标准，在测试时需根据指定的覆盖标准确定测试数据。

**参考答案**

（4）A

**试题（5）**

若某整数的 16 位补码为 $FFFF_H$（H 表示十六进制），则该数的十进制值为__（5）__。

（5）A．0 B．−1 C．$2^{16}–1$ SD．$–2^{16}+1$

**试题（5）分析**

本题考查数据表示基础知识。

根据补码定义，数值 X 的补码记作 $[X]_{补}$，如果机器字长为 $n$，则最高位为符号位，

0 表示正号，1 表示负号，正数的补码与其原码和反码相同，负数的补码则等于其反码的末尾加 1。

16 位补码能表示的数据范围为$[-2^{15}, 2^{15}, -1]$。对于整数（$2^{16}-1$）和（$-2^{16}+1$），数据表示需要 16 位，再加一个符号位，共 17 位，因此不在其 16 位补码能表示的数据范围之内。

在补码表示中，0 有唯一的编码：$[+0]_补=0\ 000000000000000$，$[-0]_补=0\ 000000000000000$，即 $0000_H$。

$[-1]_原=1\ 000000000000001$，$[-1]_反=1111111111111110$，因此 $-1$ 的补码为 $[-1]_补=1111111111111111$=FFFF。

**参考答案**

（5）B

**试题（6）**

若在系统中有若干个互斥资源 R，6 个并发进程，每个进程都需要 2 个资源 R，那么使系统不发生死锁的资源 R 的最少数目为__（6）__。

（6）A．6　　B．7　　C．9　　D．12

**试题（6）分析**

试题（6）的正确选项为 B。对于选项 A，操作系统为每个进程分配 1 个资源 R 后，若这 6 个进程再分别请求 1 个资源 R 时系统已无可供分配的资源 R，则这 6 个进程由于请求的资源 R 得不到满足而死锁。对于选项 B，操作系统为每个进程分配 1 个资源 R 后，系统还有 1 个可供分配的资源 R，能满足其中的 1 个进程的资源 R 要求并运行完毕释放占有的资源 R，从而使其他进程也能得到所需的资源 R 并运行完毕。

**参考答案**

（6）B

**试题（7）**

软件设计时需要遵循抽象、模块化、信息隐蔽和模块独立原则。在划分软件系统模块时，应尽量做到__（7）__。

（7）A．高内聚高耦合　　B．高内聚低耦合
　　C．低内聚高耦合　　D．低内聚低耦合

**试题（7）分析**

本题考查软件设计原则的基础知识。

软件设计时需要遵循抽象、模块化、信息隐蔽和模块独立原则。耦合性和内聚性是模块独立性的两个定性标准，在划分软件系统模块时，尽量做到高内聚、低耦合，提高模块的独立性。

**参考答案**

（7）B

**试题（8）**

程序的三种基本控制结构是__（8）__。

（8）A．过程、子程序和分程序　　B．顺序、选择和重复
　　C．递归、堆栈和队列　　D．调用、返回和跳转

**试题（8）分析**

本题考查软件程序设计的基础知识。

程序的三种基本控制结构是顺序结构、选择结构和重复结构。

**参考答案**

（8）B

**试题（9）**

栈是一种按“后进先出”原则进行插入和删除操作的数据结构，因此，__（9）__必须用栈。

（9）A．实现函数或过程的递归调用及返回处理时
　　B．将一个元素序列进行逆置
　　C．链表结点的申请和释放
　　D．可执行程序的装入和卸载

**试题（9）分析**

本题考查数据结构基础知识。

栈是一种后进先出的数据结构。将一个元素序列逆置时，可以使用栈也可以不用。链表结点的申请和释放次序与应用要求相关，不存在“先申请后释放”的操作要求。可执行程序的装入与卸载，也不存在“后进先出”的操作要求。对于函数的递归调用与返回，一定是后被调用执行的先返回。

**参考答案**

（9）A

**试题（10）**

两个以上的申请人分别就相同内容的计算机程序的发明创造，先后向国务院专利行政部门提出申请，__（10）__可以获得专利申请权。

（10）A．所有申请人均　　B．先申请人　　C．先使用人　　D．先发明人

**试题（10）分析**

本题考查知识产权基本知识，即专利管理部门授予专利权的基本原则。

我国授予专利权采用先申请原则，即两个以上的申请人分别就同一项发明创造申请专利权的，专利权授予最先申请的人。如果两个以上申请人在同一日分别就同样的发明创造申请专利的，应当在收到专利行政管理部门的通知后自行协商确定申请人。如果协商不成，专利局将驳回所有申请人的申请，即所有申请人均不能取得专利权。所以，先申请人可以获得专利申请权。

**参考答案**

（10）B

**试题（11）**

第三层交换根据__（11）__对数据包进行转发。

（11）A．MAC 地址　　B．IP 地址　　C．端口号　　D．应用协议

**试题（11）分析**

第三层交换是利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换与路由不同，前者用硬件实现，速度快，而后者由软件实现，速度慢。三层交换机的工作原理可以概括为：一次路由，多次交换。也就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住 MAC 目标地址和源地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧时就直接进行交换了，不再调用路由功能。所以三层交换机是按照 IP 地址选择路由，但是比通常的路由器转发的更快。

IETF 开发的多协议标记交换 MPLS（Multiprotocol Label Switching，RFC 3031）简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层协议，标准格式如下图所示。

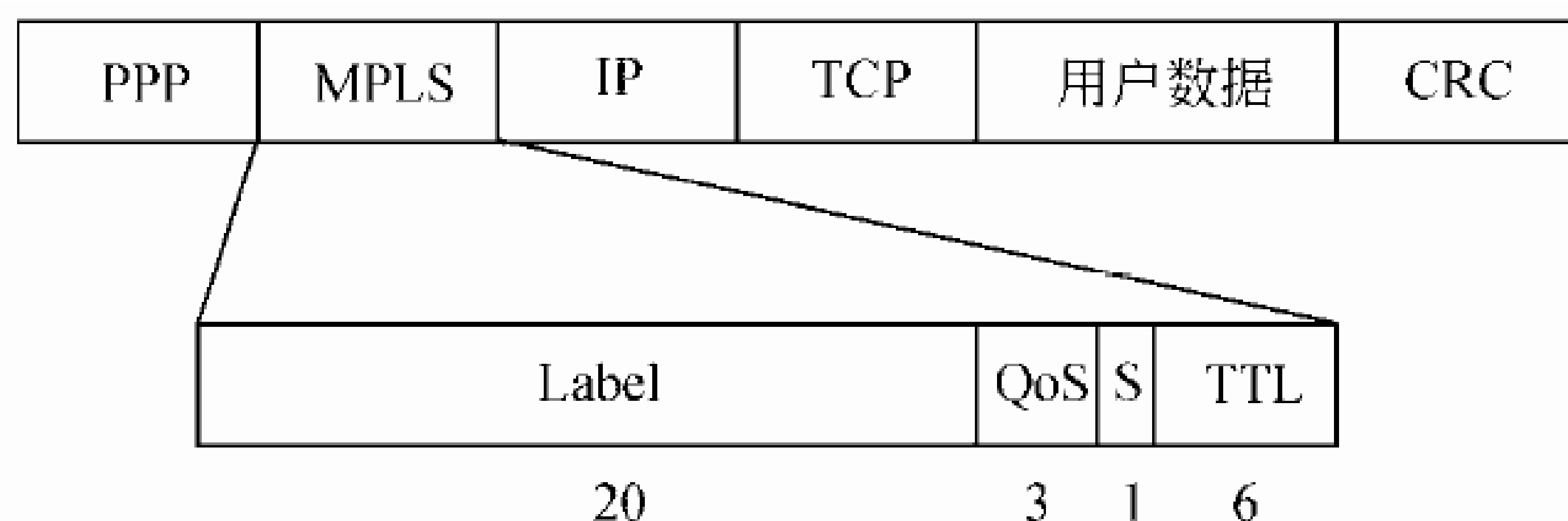



图　MPLS 头部

当带有 MPLS 标记的分组到达路由器时，标记被作为虚电路表的索引用来选择转发路径，同时路由器还可能加入新的标记。为了在另外一端能够区分，标记在每一跳步中必须重新映像，就像在虚电路网络中随着分组在子网之间转发不断改变连接标识一样。

**参考答案**

（11）B

**试题（12）**

按照 IEEE 802.1d 协议，当交换机端口处于__（12）__状态时，既可以学习 MAC 帧中的源地址，又可以把接收到的 MAC 帧转发到适当的端口。

（12）A．阻塞（blocking）　　B．学习（learning）

C．转发（forwarding）　　D．监听（listening）

**试题（12）分析**

按照IEEE 802.1d协议，所有网桥可能处于下列5种状态之一：

- 阻塞（blocking）：MAC端口不参与帧转发，也不能学习接收帧的MAC地址，仅监听进入的BPDU。
- 监听（listening）：网桥能够识别根网桥，并且可以区分根端口、指定端口和非指定端口，但不能学习接收帧的地址。
- 学习（learning）：MAC端口能够学习接收帧的MAC地址，但还不能进行转发。
- 转发（forwarding）：MAC端口可以学习接收帧的源地址，并且可以根据目标地址将其转发到适当的端口。
- 禁用（disabled）：MAC端口不参与生成树算法。

**参考答案**

（12）C

**试题（13）**

以下关于帧中继网的叙述中，错误的是__（13）__。

（13）A．帧中继提供面向连接的网络服务

B．帧在传输过程中要进行流量控制

C．既可以按需提供带宽，也可以适应突发式业务

D．帧长可变，可以承载各种局域网的数据帧

**试题（13）分析**

帧中继在第二层建立虚电路，因而第三层被简化掉了。同时，帧中继的第二层比HDLC操作简单，只进行检错而不再重传，没有滑动窗口式的流控，只有拥塞控制。

帧中继网络提供虚电路业务。虚电路是端到端的连接，不同的数据链路连接标识符（DLCI）代表不同的虚电路。虚电路分为永久虚电路（PVC）和交换虚电路（SVC）。PVC是在两个端用户之间建立的固定逻辑连接，为用户提供约定的服务。SVC是临时建立的虚电路，通过ISDN信令来建立和释放连接。

在帧中继的虚电路上可以提供不同的服务质量，网络应该保证用户以等于或低于约定数据速率CIR的速率正常传送数据。对于超过CIR的部分，一般也能可靠地传送，但是若出现网络拥塞，则会被优先丢弃。

在帧中继网上，用户的数据速率可以在一定的范围内变化，从而既可以适应流式业务，又可以适应突发式业务，这使得帧中继成为远程传输的理想形式。

**参考答案**

（13）B

**试题（14）**

在地面上相隔2000km的两地之间通过卫星信道传送4000比特长的数据包，如果数据速率为64kb/s，则从开始发送到接收完成需要的时间是__（14）__。

（14）A．48ms　　B．640ms　　C．322.5ms　　D．332.5ms

**试题（14）分析**

卫星信道的传输延迟为 270ms，4000 比特数据包发送时间为 4000b / 64kb/s=62.5ms，二者相加 270+62.5=332.5ms。

**参考答案**

（14）D

**试题（15）、（16）**

同步数字系列（SDH）是光纤信道的复用标准，其中最常用的 STM-1(OC-3)的数据速率是＿（15）＿，STM-4(OC-12)的数据速率是＿（16）＿。

（15）A．155.520 Mb/s　　B．622.080 Mb/s
　　C．2488.320 Mb/s　　D．10Gb/s

（16）A．155.520 Mb/s　　B．622.080 Mb/s
　　C．2488.320 Mb/s　　D．10Gb/s

**试题（15）、（16）分析**

同步数字系列 SDH（Synchronous Digital Hierarchy）中最常用的是 STM-1(155.520 Mb/s)、STM-4(622.080 Mb/s)、STM-16 (2488.320 Mb/s)和 STM-64 (10Gb/s)，参见下表。

**表　SONET 多路复用的速率**

| Optical Level | Electrical Level | Line Rate (Mb/s) | Payload Rate (Mb/s) | Overhead Rate (Mb/s) | SDH Equivalent | 常用近似值 |
|---|---|---|---|---|---|---|
| OC-1 | STS-1 | 51.840 | 50.112 | 1.728 | - | |
| OC-3 | STS-3 | 155.520 | 150.336 | 5.184 | STM-1 | 155Mb/s |
| OC-9 | STS-9 | 466.560 | 451.008 | 15.552 | STM-3 | |
| OC-12 | STS-12 | 622.080 | 601.344 | 20.736 | STM-4 | 622Mb/s |
| OC-18 | STS-18 | 933.120 | 902.016 | 31.104 | STM-6 | |
| OC-24 | STS-24 | 1244.160 | 1202.688 | 41.472 | STM-8 | |
| OC-36 | STS-36 | 1866.240 | 1804.032 | 62.208 | STM-13 | |
| OC-48 | STS-48 | 2488.320 | 2405.376 | 82.944 | STM-16 | 2.5Gb/s |
| OC-96 | STS-96 | 4976.640 | 4810.752 | 165.888 | STM-32 | |
| OC-192 | STS-192 | 9953.280 | 9621.504 | 331.776 | STM-64 | 10Gb/s |

**参考答案**

（15）A　（16）B

**试题（17）**

采用 CRC 进行差错校验，生成多项式为 $G(X)=X^4+X+1$，信息码字为 10111，则计算出的 CRC 校验码是＿（17）＿。

（17）A．0000　　B．0100　　C．0010　　D．1100

**试题（17）分析**

$G(X)=X^4+X+1$ 对应的二进制序列为 10011，循环冗余校验码的计算方法（即进行“按位异或”运算）如下：

```
  101110000
  10011
-----------
  001000000
    10011
-----------
    0001100
```

**参考答案**

（17）D

**试题（18）**

数字用户线（DSL）是基于普通电话线的宽带接入技术，可以在铜质双绞线上同时传送数据和话音信号。下列选项中，数据速率最高的 DSL 标准是__（18）__。

（18）A．ADSL　　B．VDSL　　C．HDSL　　D．RADSL

**试题（18）分析**

数字用户线（Digital Subscriber Line，DSL）是基于普通电话线的宽带接入技术，可以在一对铜质双绞线上同时传送数据和话音信号。DSL 有多种模式，统称为 xDSL。

根据上、下行传输速率是否相同，可以把 DSL 划分为对称和不对称两种传输模式。对称 DSL 的上、下行传输速率相同，用于代替传统的 T1/E1 接入线路。

高数据速率用户数字线（High-data-rate DSL，HDSL）采用两对双绞线提供全双工数据传输，支持 $n\times$64kb/s（$n$=1，2，3，…）的各种速率，最高可达 1.544Mb/s 或 2.048Mb/s，传输距离可达 3～5km。HDSL 在视频会议、远程教学、移动电话基站连接等方面得到了广泛应用。

速率自适应用户数字线（Rate Adaptive DSL，RADSL）支持同步和非同步传输方式，下行速率为 640kb/s～12Mb/s，上行速率为 128kb/s～1Mb/s，也支持数据和语音同时传输。RADSL 具有速率自适应的特点，可以根据双绞线的质量和传输距离动态调整用户访问速率。RADSL 允许通信双方的 Modem 寻找流量最小的频道来传送数据，以保证一定的数据速率。RADSL 特别适用于线路质量千差万别的农村、山区等地区使用。

甚高比特率数字用户线（Very High Bit-rate DSL，VDSL）可在较短的距离上获得极高的传输速率，是各种 DSL 中速度最快的一种。在一对铜质双绞线上，VDSL 的下行速率可以扩展到 52Mb/s，同时支持 1.5～2.3Mb/s 的上行速率，但传输距离只有 300～1000m。当下行速率降至 13Mb/s 时，传送距离可达到 1.5km 以上，此时上行速率为 1.6～2.3Mb/s 左右。传输距离的缩短，会使码间干扰大大减少，数字信号处理过程就大为简化，所以其设备成本要比 ADSL 低。

ADSL（Asymmetrical Digital Subscriber Line）是一种非对称 DSL 技术，在一对铜线上可提供 512kb/s～1Mb/s 的上行速率和 1～8Mb/s 的下行速率，有效传输距离为 3～5km 左右。ADSL 在进行数据传输的同时还可以使用第三个信道提供 4kHz 的语音传输。现在比较成熟的 ADSL 标准有两种，即 G.DMT 和 G.Lite。G.DMT 是全速率的 ADSL 标准，支持 8Mb/s 的下行速率及 1.5Mb/s 的上行速率，但 G.DMT 要求用户端安装 POTS 分离器，技术复杂而且价格昂贵。G.Lite 标准速率较低，下行速率为 1.5Mb/s，上行速率为 512kb/s，但省去了 POTS 分离器，成本较低且便于安装。G.DMT 较适用于小型办公室（SOHO）应用，而 G.Lite 则更适用于普通家庭应用。

**参考答案**

（18）B

**试题（19）**

下列 FTTx 组网方案中，光纤覆盖面最广的是＿（19）＿。

（19）A．FTTN　　B．FTTC　　C．FTTH　　D．FTTZ

**试题（19）分析**

光纤接入网（Optical Access Network，OAN）又称光纤用户环路（Fiber in the loop，FITL），其结构如下图所示。

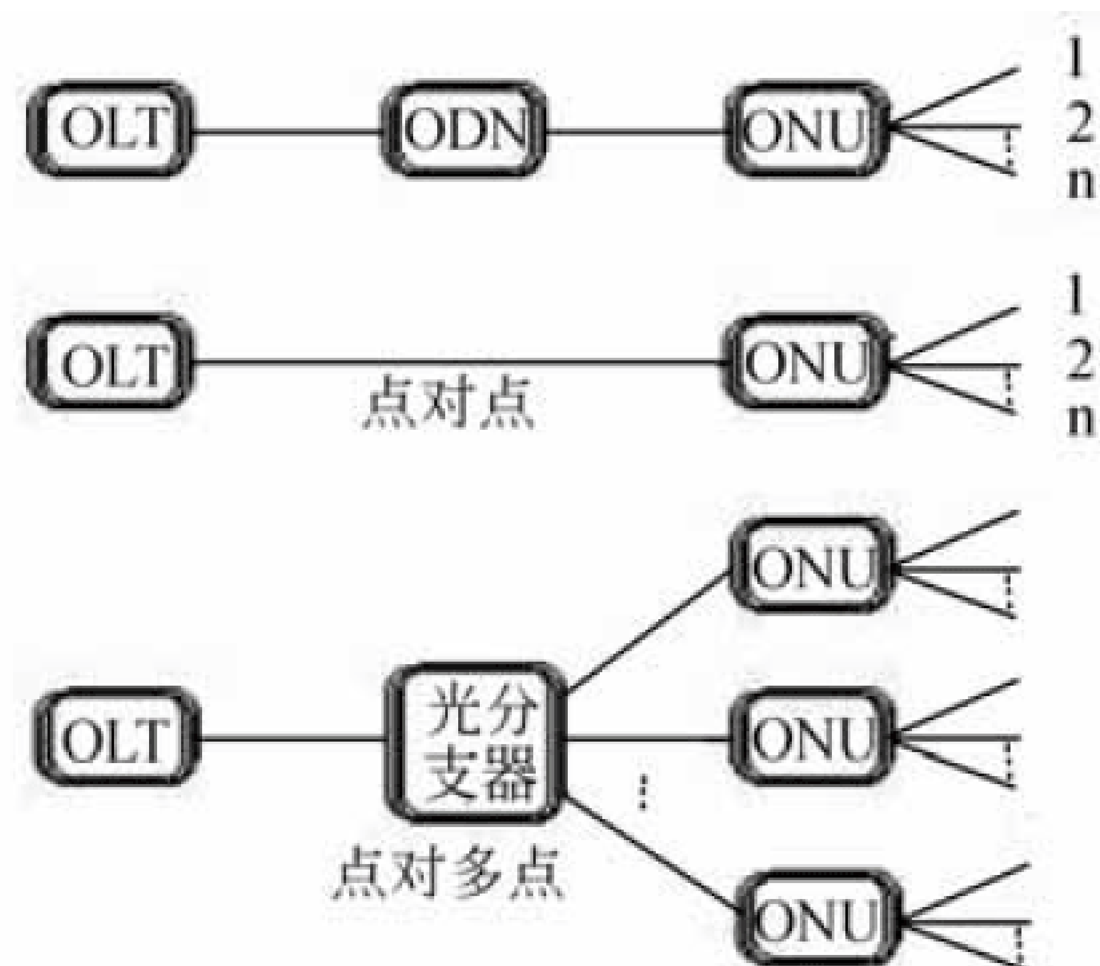



图　光纤接入一般结构

在交换局中设有光纤线路终端设备（Optical Line Terminal，OLT），在用户侧安装光纤网络单元（Optical Network Unit，ONU），OLT 和 ONU 之间则是光纤配线网（Optical Distribution Network，ODN）。ODN 可采用多种拓扑结构，例如点对点或点到多点方式。在点对多点的连接方式中，从 OLT 出来的光纤信号通过光分路器或星型耦合器传送到多个 ONU 上，这种方式被称为双星结构。ONU 采用星型拓扑连接多个用户，传输介质可以是同轴电缆或双绞铜线。根据 ONU 所在位置以及 ONU 与用户的距离，FITL 可分为多种形式，统称为 FTTx（Fiber-to-the-x），如下表所示。

**表　光纤接入网的分类**

| 分　　类 | 含　　义 | 功　　能 |
|---|---|---|
| FTTH（Fiber To The Home） | 光纤到户 | 主要为家庭用户提供服务，ONU 放置在用户家中 |
| FTTD（Fiber To The DeskTop） | 光纤到桌面 | 主要为家庭用户提供服务，ONU 放置在用户桌面 |
| FTTC（Fiber To The Curb）） | 光纤到路边 | 主要为住宅用户提供服务，ONU 放置在路边 |
| FTTB（Fiber To The Building） | 光纤到大楼 | 主要为公寓用户提供服务，ONU 放置在楼内 |
| FTTO（Fiber To The Office）） | 光纤到办公室 | 主要为企事业单位用户提供服务，ONU 位于办公室或楼层 |
| FTTF（Fiber To The Feeder） | 光纤到楼层 | |
| FTTN（Fiber To The Node） | 光纤到节点 | 光纤延伸到电缆交接箱所在处，可以覆盖 200～300 用户 |
| FTTZ（Fiber To The Zone） | 光纤到小区 | 用于 HFC，ONU 位于居民小区 |

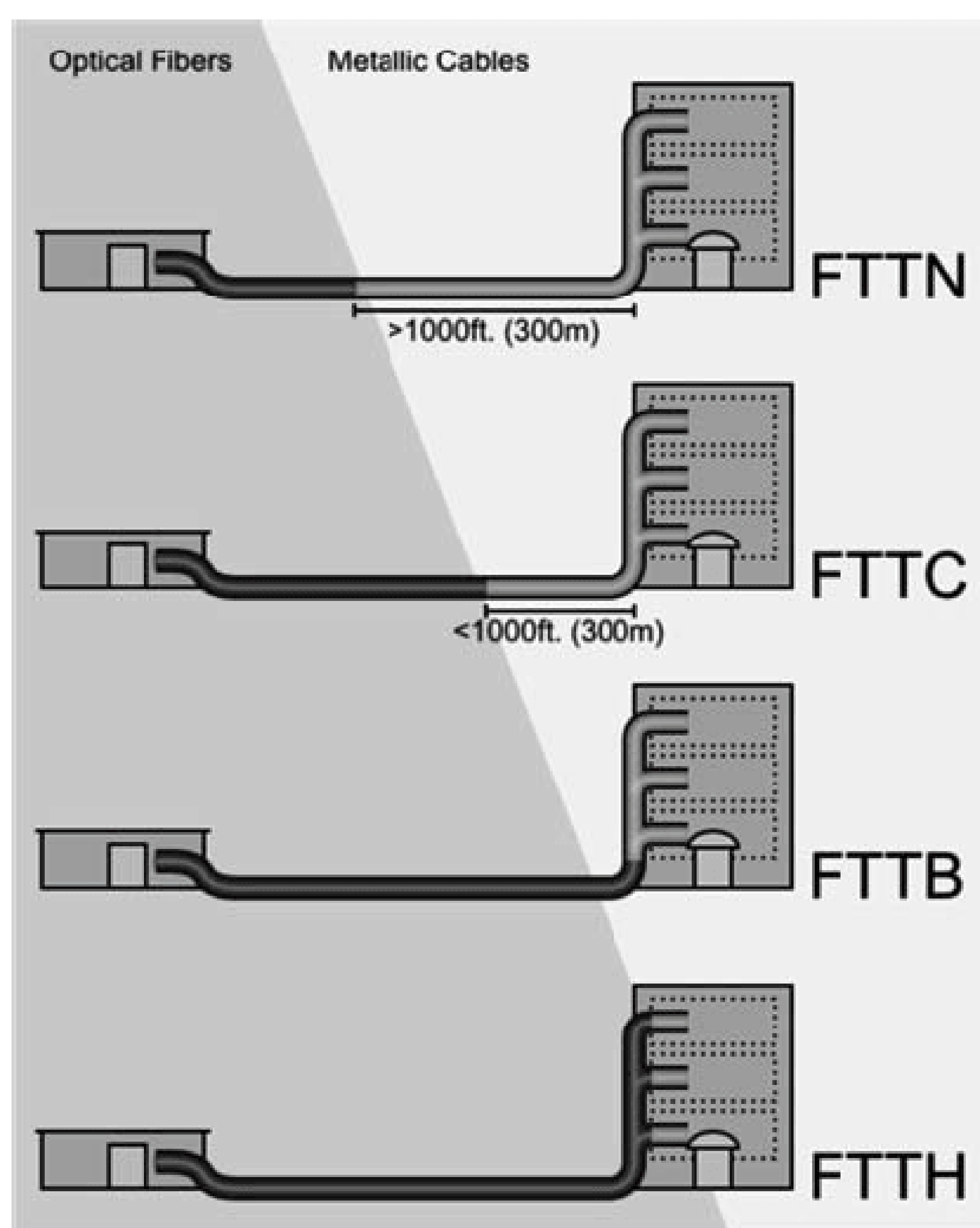



图　各种 FTTx 的比较

上图表示光纤与用户终端之间距离的变化情况，左边是电信中心局，与光纤连接；右边是连接电信网络的用户住所，其中的虚线方框表示同一建筑物内的用户家庭或办公室，与铜缆相连。可以看出，对于 FTTN，光纤网离用户终端最远，而在 FTTH 中，光纤可以直接连接到用户桌面。FTTH 比 FTTN 建设成本高，光纤覆盖面更广，用户可以获得更高的带宽，因此在高端用户小区建设方面具有一定的优势。然而，FTTN 可以有效降低光纤接入的成本，运营维护比较方便，是普通居民社区的理想接入方案。

**参考答案**

（19）C

**试题（20）、（21）**

网络地址和端口翻译（NAPT）用于__（20）__，这样做的好处是__（21）__。

（20）A．把内部的大地址空间映射到外部的小地址空间
B．把外部的大地址空间映射到内部的小地址空间
C．把内部的所有地址映射到一个外部地址
D．把外部的所有地址映射到一个内部地址

（21）A．可以快速访问外部主机
B．限制了内部对外部主机的访问
C．增强了访问外部资源的能力
D．隐藏了内部网络的 IP 配置

**试题（20）、（21）分析**

网络地址翻译（Network Address Translation，NAT）技术主要解决 IP 地址短缺问题，最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。局部地址是在子网内部独立编址的，可以与外部地址重叠。这种想法的基础是假定在任何时候子网中只有少数计算机需要与外部通信，可以让这些计算机共享少量的全局 IP 地址。后来根据这种技术又开发出其他一些应用。

首先是动态地址翻译（Dynamic Address Translation）技术。所谓存根域（Stub Domain）是内部网络的抽象，任何时候存根域内只有一部分主机要与外界通信，所以整个存根域只需共享少量的全局 IP 地址。存根域有一个边界路由器，由它来处理域内与外部的通信。我们假定：

- $m$：内部地址数。
- $n$：全局地址数（NAT 地址）。

当 $m \geqslant 1$ 并且 $m \geqslant n$ 时，可以把大的地址空间映像到小的地址空间。所有 NAT 地址放在一个缓冲区中，并在存根域的边界路由器中建立一个内部地址和全局地址的动态映像表，用以把内部地址翻译成全局地址。动态地址翻译的好处是节约了全局 IP 地址，而且不需要改变子网内部的配置。

另外一种特殊的 NAT 应用是 $m$:1 翻译，这种技术也叫作地址伪装（Masquerading），因为用一个全局 IP 地址就可以把子网中所有主机的 IP 地址隐藏起来。如果子网中有多个主机要同时通信，那么还要对端口号进行翻译，所以这种技术经常被称为网络地址和端口翻译（Network Address Port Translation，NAPT）。在很多 NAPT 实现中专门保留一部分端口号给地址伪装使用，叫作伪装端口号。这种方法有如下特点：

- 出口分组的源地址被路由器的外部 IP 地址代替，出口分组的源端口号被一个未使用的伪装端口号代替。
- 如果进来的分组的目标地址是本地路由器的 IP 地址，而目标端口号是路由器的伪装端口号，则 NAT 路由器就检查是否为伪装会话，并试图通过伪装表对 IP 地址和端口号进行翻译。

伪装技术可以作为一种安全手段使用，借以限制外部对内部主机的访问。另外还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。

**参考答案**

（20）C （21）D

**试题（22）、（23）**

边界网关协议BGP的报文__（22）__传送。一个外部路由器通过发送__（23）__报文与另一个外部路由器建立邻居关系，如果得到应答，才能周期性地交换路由信息。

（22）A. 通过TCP连接 B. 封装在UDP数据报中
C. 通过局域网 D. 封装在ICMP包中

（23）A. Update B. Keepalive
C. Open D. 通告

**试题（22）、（23）分析**

通用的外部网关协议是边界网关协议（Border Gateway Protocol，BGP）第4版。运行这个协议的网关向对等实体（Peer）发布可以到达的AS列表。通过交换路由信息，网关可以建立所有AS的互连结构图，并根据路由决策算法对环路进行修剪。

BGP4发布的路由信息是可到达网络的IP地址前缀，并支持CIDR技术，通过路由汇聚功能形成超级网络，以简化路由表，并提高转发速度。

BGP4报文通过TCP连接传送，其报文类型有建立邻居关系的OPEN报文，对OPEN请求进行应答的KEEPALIVE报文，发送路由更新信息的UPDATE报文，以及通告路由错误的NOTIFICATION报文。

BGP的有限状态机如下图所示，共有13个BGP事件，引起BGP协议机在6个状态之间转换。

**参考答案**

（22）A （23）C

**试题（24）**

在IPv6中，地址类型是由格式前缀来区分的。IPv6可聚合全球单播地址的格式前缀是__（24）__。

（24）A. 001 B. 1111 1110 10 C. 1111 1110 11 D. 1111 1111

**试题（24）分析**

IPv6地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，用类似于IPv4 CIDR的方法可表示为“IPv6地址/前缀长度”的形式。例如结点地址如下：

12AB:0:0:CD30:123:4567:89AB:CDEF

若其子网号为

12AB:0:0:CD30::/60

则等价的写法是

12AB:0:0:CD30:123:4567:89AB:CDEF/60

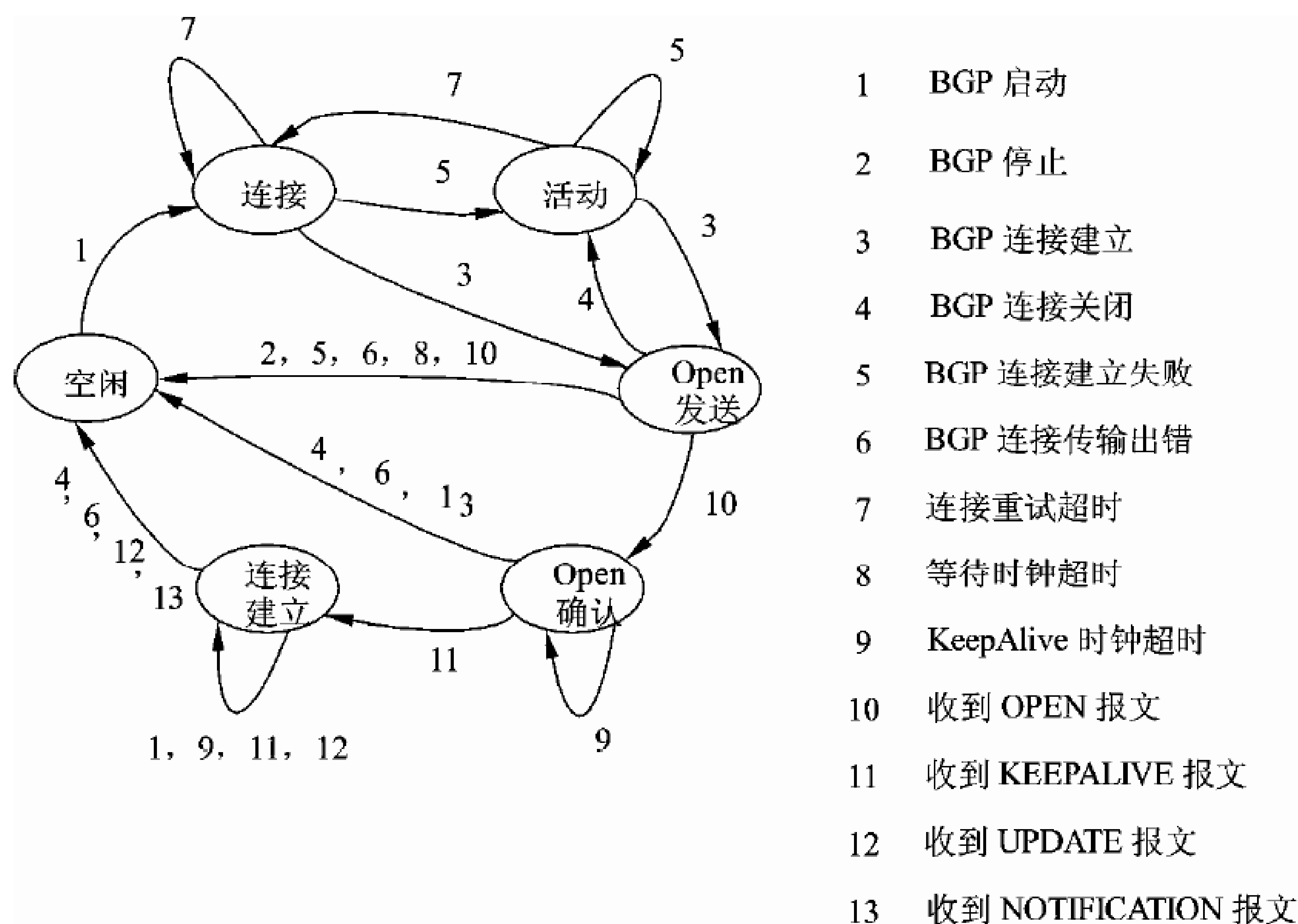



图　BGP 的有限状态机

IPv6 单播地址包括可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

① 可聚合全球单播地址：这种地址在全球范围内有效，相当于 IPv4 公用地址。全球地址的设计有助于构架一个基于层次的路由基础设施。可聚合全球单播地址结构如下图所示。

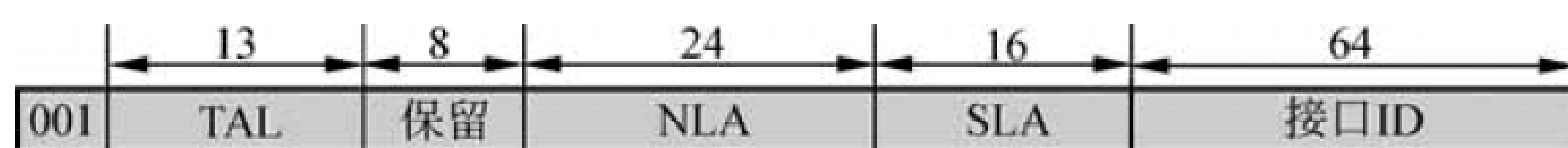



图　可聚合全球单播地址

可聚合全球单播地址格式前缀为 001，随后的顶级聚合体 TLA（Top Level Aggregator）、下级聚合体 NLA（Next Level Aggregator）以及站点级聚合体 SLA（Site Level Aggregator）构成了自顶向下的 3 级路由层次结构。TLA 是远程服务供应商的骨干网接入点，TLA 向地区互联网注册机构 RIR（ARIN、RIPE NCC、APNIC 等）申请 IPv6 地址块，TLA 之下就是商业地址分配范围。NLA 是一般的 ISP，它们把从 TLA 申请的地址分配给 SLA，各个站点级聚合体再为机构用户或个人用户分配地址。分层结构的最底层是主机接口，通常是在主机的 48 位 MAC 地址前面填充 0xFFFE 构成的接口 ID。

② 本地单播地址：这种地址的有效范围仅限于本地，又分为两类：

- 链路本地地址：其格式前缀为 1111 1110 10，用于同一链路的相邻结点间的通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址（APIPA），可用于邻居发现，并且总是自动配置的，包含链路本地地址的分组不会被路由器转发。
- 站点本地地址：其格式前缀为 1111 1110 11，相当于 IPv4 中的私网地址。如果企业内部网没有连接到 Internet 上，则可以使用这种地址。站点本地地址不能被其他站点访问，包含这种地址的分组也不会被路由器转发到站点之外。

③ 组播地址 ：IPv6 组播可以将数据报传输给组内所有成员。IPv6 组播地址格式前缀为 1111 1111，此外还包括标志（Flags）、范围和组 ID 等字段，如下图所示。

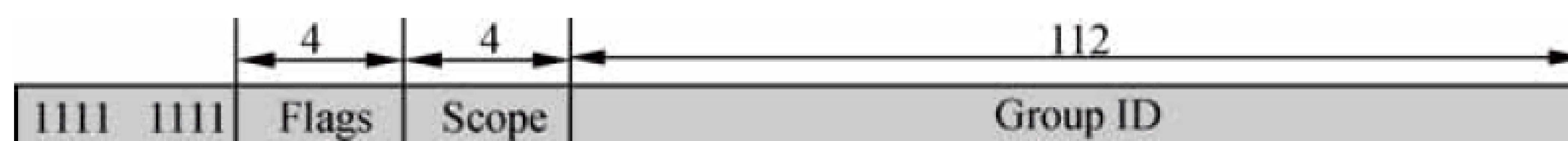



图　IPv6 组播地址

Flags 可表示为 000T，T=0 表示被 IANA 永久分配的组播地址；T=1 表示临时的组播地址。Scope 是组播范围字段，下表列出了在 RFC 2373 中定义的 Scope 的值。Group ID 标识了一个给定范围内的组播组。永久分配的组播组 ID 与范围字段无关，临时分配的组播组 ID 在特定的范围内有效。

**表　Scope 字段值**

| 值 | 范围 |
|---|---|
| 0 | 保留 |
| 1 | 结点本地范围 |
| 2 | 链路本地范围 |
| 5 | 站点本地范围 |
| 8 | 机构本地范围 |
| E | 全球范围 |
| F | 保留 |

④ 任意播地址：任意播地址仅用做目标地址，且只能分配给路由器。任意播地址是在单播地址空间中分配的。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。为构造一个子网-路由器任意播地址，子网前缀必须固定，其余位置全“0”，见下图。




图　子网-路由器任意播地址

下表是对 IPv4 与 IPv6 地址的比较。

**表　IPv4 和 IPv6 地址比较**

| IPv4 地址 | IPv6 地址 |
|---|---|
| 点分十进制表示 | 带冒号的十六进制表示，0 压缩 |
| 分为 A、B、C、D、E 等 5 类 | 不分类 |
| 组播地址 224.0.0.0/4 | 组播地址 FF00::/8 |
| 广播地址（主机部分为全 1） | 任意播（限于子网内部） |
| 默认地址 0.0.0.0 | 不确定地址:: |
| 回环地址 127.0.0.1 | 回环地址::1 |
| 公共地址 | 可聚合全球单播地址 FP＝001 |
| 私网地址 10.0.0.0/8;<br>172.16.0.0/12; 192.168.0.0/16 | 站点本地地址 FECO::/48 |
| 自动专用 IP 地址 169.254.0.0/16 | 链路本地地址 FE8O::/48 |

**参考答案**

（24）A

**试题（25）、（26）**

在 IPv6 的单播地址中有两种特殊地址，其中地址 0:0:0:0:0:0:0:0 表示__（25）__，地址 0:0:0:0:0:0:0:1 表示__（26）__。

（25）A．不确定地址，不能分配给任何结点

B．回环地址，结点用这种地址向自身发送 IPv6 分组

C．不确定地址，可以分配给任何结点

D．回环地址，用于测试远程结点的连通性

（26）A．不确定地址，不能分配给任何结点

B．回环地址，结点用这种地址向自身发送 IPv6 分组

C．不确定地址，可以分配给任何结点

D．回环地址，用于测试远程结点的连通性

**试题（25）、（26）分析**

IPv6 地址有单播地址、任意播地址和组播地址三种类型：

（1）单播（Unicast）地址。

单播地址是单个网络接口的标识符。对于有多个接口的结点，其中任何一个单播地址都可以用作该结点的标识符。但是为了满足负载平衡的需要，在 RFC 2373 中规定，只要在实现中多个接口看起来形同一个接口就允许这些接口使用同一地址。IPv6 的单播地址是用一定长度的格式前缀汇聚的地址，类似于 IPv4 中的 CIDR 地址。单播地址中有下列两种特殊地址：

- 不确定地址：地址 0:0:0:0:0:0:0:0 称为不确定地址，不能分配给任何结点。不确

定地址可以在初始化主机时使用，在主机未取得地址之前，它发送的 IPv6 分组中的源地址字段可以使用这个地址。这种地址不能用作目标地址，也不能用在 IPv6 路由头中。

- 回环地址：地址 0:0:0:0:0:0:0:1 称为回环地址，结点用这种地址向自身发送 IPv6 分组。这种地址不能分配给任何物理接口。

（2）任意播（AnyCast）地址。

这种地址表示一组接口（可属于不同结点的）的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对 IPv6 任意播地址存在下列限制：

- 任意播地址不能用作源地址，而只能作为目标地址。
- 任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

（3）组播（MultiCast）地址。

组播地址是一组接口（一般属于不同结点）的标识符，发往组播地址的分组被传送给该地址标识的所有接口。IPv6 中没有广播地址，它的功能已被组播地址所代替。

在 IPv6 地址中，任何全“0”和全“1”字段都是合法的，除非特别排除的之外。特别是前缀可以包含“0”值字段，也可以用“0”作为终结字段。一个接口可以被赋予任何类型的多个地址（单播、任意播、组播）或地址范围。

**参考答案**

（25）A （26）B

**试题（27）**

Telnet 采用客户端/服务器工作方式，采用__（27）__格式实现客户端和服务器的数据传输。

（27）A. NTL B. NVT C. base-64 D. RFC 822

**试题（27）分析**

本题考查 Telnet 文件传输格式。Telnet 采用客户机/服务器工作方式。用户终端运行 Telnet 客户程序，远程主机运行 Telnet 服务器程序。Telnet 定义了网络虚拟终端 NVT（Network Virtual Terminal）。NVT 代码包括标准的 7 单位 ASCII 字符集和 Telnet 命令集。这些字符和命令提供了本地终端和远程主机之间的网络接口。

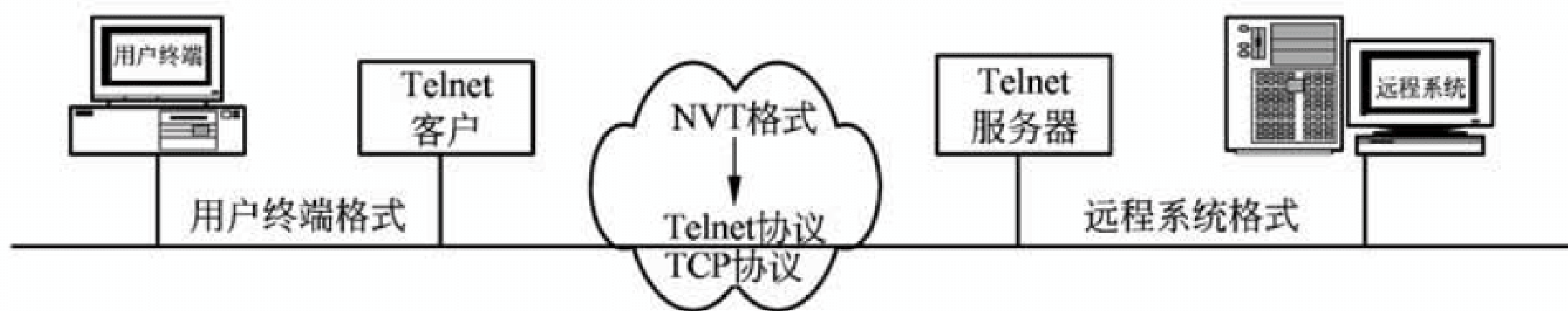
客户机与服务器程序之间执行 Telnet NVT 协议，而在两端则分别执行各自的操作系统功能，如下页图所示。

**参考答案**

（27）B

**试题（28）**

以下关于 DNS 服务器的叙述中，错误的是__（28）__。




Telnet 客户机/服务器概念模型示意图

（28）A．用户只能使用本网段内 DNS 服务器进行域名解析

B．主域名服务器负责维护这个区域的所有域名信息

C．辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务

D．转发域名服务器负责非本地域名的查询

**试题（28）分析**

本题考查 DNS 的几种服务器形式。

主域名服务器（primary name server）负责维护这个区域的所有域名信息，是特定域所有信息的权威性信息源。当主域名服务器关闭、出现故障或负载过重时，辅域名服务器（secondary name server）作为备份服务器提供域名解析服务。辅助服务器从主域名服务器获得授权，并定期向主服务器询问是否有新数据，如果有则调入并更新域名解析数据，以达到与主域名服务器同步的目的。缓存域名服务器（caching-only server）可运行域名服务器软件但是没有域名数据库。它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就予以回答。转发域名服务器（forwarding server）负责所有非本地域名的本地查询。转发域名服务器接到查询请求时，在其缓存中查找，如找不到就把请求依次转发到指定的域名服务器，直到查询到结果为止，否则返回无法映射的结果。

用户可以通过中继代理使用外网段内 DNS 服务器进行域名解析，故选 A。

**参考答案**

（28）A

**试题（29）**

以下域名服务器中，没有域名数据库的是＿（29）＿。

（29）A．缓存域名服务器　　B．主域名服务器

C．辅域名服务器　　D．转发域名服务器

**试题（29）分析**

本题考查 DNS 的域名数据库。

缓存域名服务器从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就予以回答。因此缓存域名服务器没有域名数据库。故选 A。

**参考答案**

（29）A

**试题（30）**

通过“Internet 信息服务（IIS）管理器”管理单元可以配置 FTP 服务，若将控制端口设置为 2222，则数据端口自动设置为 （30） 。

（30）A．20　　B．80　　C．543　　D．2221

**试题（30）分析**

客户端向服务器的 FTP 端口发送连接请求，服务器接受连接，建立一条命令链路。当需要传送数据时，服务器从另一端口向客户端的空闲端口发送连接请求，建立一条数据链路来传送数据。默认情况下控制端口为 21，数据端口为 20，但数据端口和控制端口都可以人为设置。若将控制端口重新设置，则数据端口自动设置为数据端口–1。

因此，若将控制端口设置为 2222，则数据端口自动设置为 2221，正确答案为 D。

**参考答案**

（30）D

**试题（31）～（33）**

在一台 Apache 服务器上通过虚拟主机可以实现多个 Web 站点。虚拟主机可以是基于 （31） 的虚拟主机，也可以是基于名字的虚拟主机。若某公司创建名字为 www.business.com 的虚拟主机，则需要在 （32） 服务器中添加地址记录。在 Linux 中该地址记录的配置信息如下，请补充完整。

```
NameVirtualHost 192.168.0.1
<VirtualHost 192.168.0.1>
    (33)   www.business.com
    DocumentRoot /var/www/html/business
</VirtualHost>
```

（31）A．IP　　B．TCP　　C．UDP　　D．HTTP

（32）A．SNMP　　B．DNS　　C．SMTP　　D．FTP

（33）A．WebName　　B．HostName　　C．ServerName　　D．WWW

**试题（31）～（33）分析**

本题考查 APACHE 虚拟主机方面的相关知识。

Apache 服务器可提供基于 IP 的虚拟主机或者基于名字的虚拟主机，服务器构建好之后，需要在 DNS 记录中添加对应的地址记录，从而其他用户可通过域名进行访问，ServerName 选项用于设置服务器用于辨识自己的主机信息。

**参考答案**

（31）A　（32）B　（33）C

**试题（34）**

ATM 高层定义了 4 类业务，压缩视频信号的传送属于 （34） 类业务。

（34）A．CBR　　B．VBR　　C．UBR　　D．ABR

**试题（34）分析**

本题考查 ATM 的业务类别知识。

ATM 高层与业务相关，ATM4.0 规定的用户业务分为 4 类。其中 CBR（Constant Bit Rate）采用固定比特率业务适合于交互式话音和视频流。VBR（Variable Bit Rate）可变比特率业务适合交互式压缩视频信号（MPEG）。ABR（Available Bit Rate）采用有效比特率业务，用于突发式通信。UBR（Unspecified Bit Rate）为不定比特率，可用于传送 IP 分组，包括文件传输，电子邮件和 USENET 新闻是这类业务潜在的应用领域。

故压缩视频信号的传送属于 CBR 类业务，选 B。

**参考答案**

（34）B

**试题（35）**

某 Linux DHCP 服务器 dhcpd.conf 的配置文件如下：

```
ddns-update-style none;
subnet 192.168.0.0 netmask 255.255.255.0{
range 192.168.0.200 192.168.0.254;
ignore client-updates;
default-lease-time 3600;
max-lease-time 7200;
option routers 192.168.0.1;
option domain-name"test.org";
option domain-name-servers 192.168.0.2;
 }
host test1{ hardware ethernet  00:E0:4C:70:33:65;fixed-address  192.168.0.8;}
```

客户端 IP 地址的默认租用期为＿（35）＿小时。

（35）A．1　　B．2　　C．60　　D．120

**试题（35）分析**

本题考查 Linux DHCP 服务器的配置。

配置文件中 default-lease-time 3600 表明客户端 IP 地址的默认租用期为 3600 秒，即 1 小时；max-lease-time 7200 表明客户端 IP 地址的最大租用期为 7200 秒，即 2 小时。故选 A。

**参考答案**

（35）A

**试题（36）**

DHCP 客户端不能从 DHCP 服务器获得＿（36）＿。

（36）A．DHCP 服务器的 IP 地址　　B．Web 服务器的 IP 地址

C．DNS 服务器的 IP 地址　　　　D．默认网关的 IP 地址

**试题（36）分析**

本题考查 DHCP 服务器的配置。

DHCP 客户端不能从 DHCP 服务器获得 DHCP 服务器的 IP 地址、DNS 服务器的 IP 地址、默认网关的 IP 地址等，从下图中即可看出。

```
Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Realtek RTL8102E/RTL8103E Family PCI -E Fast Ethernet NIC
    Physical Address. . . . . . . . . : 0E-34-54-04-88-09
    Dhcp Enabled. . . . . . . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . . . . . . . . : 112.119.113.77
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 112.119.113.254
    DHCP Server . . . . . . . . . . . : 192.168.251.10
    DNS Servers . . . . . . . . . . . : 112.119.114.3
                                        62.154.1.4
    Lease Obtained. . . . . . . . . . : 2010年2月23日 10:52:20
    Lease Expires . . . . . . . . . . : 2010年2月23日 22:52:20
```

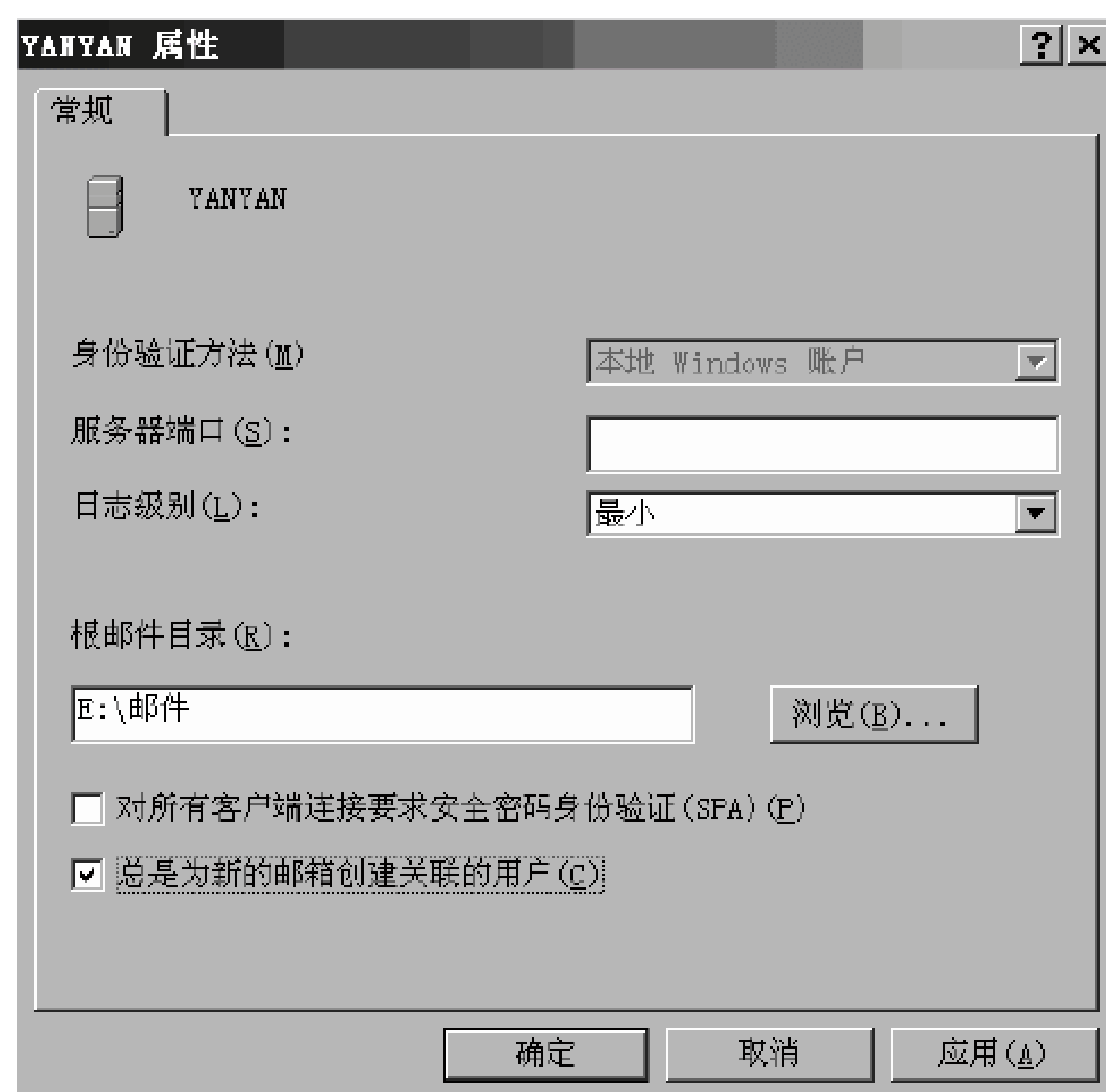
但是，不能获得 Web 服务器的 IP 地址。故选 B。

**参考答案**

（36）B

**试题（37）**

配置 POP3 服务器时，邮件服务器的属性对话框如下图所示，其中默认情况下“服务器端口”文本框应填入__（37）__。




（37）A．21　　　B．25　　　C．80　　　D．110

**试题（37）分析**

本题考查 POP3 服务器的配置。

POP3 服务器默认端口为 110，故“服务器端口”文本框应填入 110，选 D。

**参考答案**

（37）D

**试题（38）**

在 Windows 的 DoS 窗口中键入命令

C:\> nslookup

set type=ns

> 202.30.192.2

这个命令序列的作用是__（38）__。

（38）A．查询 202.30.192.2 的邮件服务器信息

B．查询 202.30.192.2 到域名的映射

C．查询 202.30.192.2 的区域授权服务器

D．显示 202.30.192.2 中各种可用的信息资源记录

**试题（38）分析**

本题考查 nslookup 命令。Nslookup 命令用于显示 DNS 查询信息，诊断和排除 DNS 故障。

Nslookup 有交互式和非交互式两种工作方式，交互模式下，可以用 set 命令设置选项，满足指定的查询需要。DNS 服务器中主要的资源记录有 A（域名到 IP 地址的映射）、PTR（IP 地址到域名的映射）、MX（邮件服务器及其优先级）、CNAM（别名）和 NS（区域的授权服务器）等类型。故选 C。

**参考答案**

（38）C

**试题（39）**

HTTPS 采用__（39）__协议实现安全网站访问。

（39）A．SSL　　B．IPSec　　C．PGP　　D．SET

**试题（39）分析**

本题考查网络安全方面关于安全协议的基础知识。

IPSec（IP Security）是 IETF 定义的一组协议，用于增强 IP 网络的安全性。IPSec 是在网络层建立安全隧道，适用于建立固定的虚拟专用网。

PGP（Pretty Good Privacy）是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包，如今 PGP 已经成为使用最广泛的电子邮件加密软件。

SET（Secure Electronic Transaction）是一个安全协议和报文格式的集合，它融合了 Netscape 的 SSL、Microsoft 的 STT（Secure Transaction Technology）、Terisa 的S-HTTP、以及 PKI 技术，通过数字证书和数字签名机制，使得客户可以与供应商进行安全的电子交易。

SSL（Secure Socket Layer）是 Netscape 于 1994 年开发的传输层安全协议，用于实现 Web 安全通信。SSL/TLS 在 Web 安全通信中被称为 HTTPS。所以答案是 A。

**参考答案**

（39）A

**试题（40）、（41）**

杀毒软件报告发现病毒 Macro.Melissa，由该病毒名称可以推断出病毒类型是（40），这类病毒主要感染目标是 （41） 。

（40）A．文件型　　B．引导型
　　C．目录型　　D．宏病毒

（41）A．EXE 或 COM 可执行文件　　B．Word 或 Excel 文件
　　C．DLL 系统文件　　D．磁盘引导区

**试题（40）、（41）分析**

本题考查计算机病毒方面的基础知识。

计算机病毒的分类方法有许多种，按照最通用的区分方式，即根据其感染的途径以及采用的技术区分，计算机病毒可分为文件型计算机病毒、引导型计算机病毒、宏病毒和目录型计算机病毒。

文件型计算机病毒感染可执行文件（包括 EXE 和 COM 文件）。

引导型计算机病毒影响软盘或硬盘的引导扇区。

目录型计算机病毒能够修改硬盘上存储的所有文件的地址。

宏病毒感染的对象是使用某些程序创建的文本文档、数据库、电子表格等文件，从文件名可以看出 Macro.Melissa 是一种宏病毒。

**参考答案**

（40）D　（41）B

**试题（42）**

以下 ACL 语句中，含义为"允许 172.168.0.0/24 网段所有 PC 访问 10.1.0.10 中的 FTP 服务"的是（42）。

（42）A．access-list 101 deny tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp
　　B．access-list 101 permit tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp
　　C．access-list 101 deny tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp
　　D．access-list 101 permit tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

**试题（42）分析**

本题考查防火墙方面 ACL 配置的基础知识。

题中四个选项给出的是 4 条扩展 ACL 语句，扩展 ACL 语句的语法如下：

access-list [dynamic dynamic-name [timeout minutes]] {deny | permit} tcp source wildcard-mask [operator [port]] destination wildcard-mask [operator [port]] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

在 ACL 语句中，"172.168.0.0/24 网段"表示为 172.168.0.0 0.0.0.255，目标主机

10.1.0.10 表示为 host 10.1.0.10，并且源地址位于目标地址之前。所以，正确的 ACL 语句应该是选项 B。

**参考答案**

（42）B

**试题（43）**

以下关于加密算法的叙述中，正确的是<u>（43）</u>。

（43）A．DES 算法采用 128 位的密钥进行加密
　　B．DES 算法采用两个不同的密钥进行加密
　　C．三重 DES 算法采用 3 个不同的密钥进行加密
　　D．三重 DES 算法采用 2 个不同的密钥进行加密

**试题（43）分析**

本题考查网络安全方面加密算法的基础知识。

DES（Data Encryption Standard）明文被分成 64 位的块进行变换运算，变换由 56 位的密钥的不同排列形式控制，最后产生 64 位的密文块。

三重 DES（Triple-DES）是 DES 的改进算法，它使用两把密钥对报文作三次 DES 加密，第一层和第三层中使用相同的密钥，产生一个有效长度为 112 位的密钥。所以正确答案是 D。

**参考答案**

（43）D

**试题（44）**

IIS 服务支持的身份验证方法中，需要利用明文在网络上传递用户名和密码的是<u>（44）</u>。

（44）A．.NET Passport 身份验证　　B．集成 Windows 身份验证
　　C．基本身份验证　　D．摘要式身份验证

**试题（44）分析**

本题考查 Windows IIS 服务中身份认证的基础知识。

Windows IIS 服务支持的身份认证方式有四种：.NET Passport 身份验证、集成 Windows 身份验证、摘要式身份验证和基本身份验证。

集成 Windows 身份验证以 Kerberos 票证的形式通过网络向用户发送身份验证信息，并提供较高的安全级别。Windows 集成身份验证使用 Kerberos 版本 5 和 NTLM 身份验证。

摘要式身份验证，将用户凭据作为 MD5 哈希或消息摘要在网络中进行传输，这样就无法根据哈希对原始用户名和密码进行解码。

.NET Passport 身份验证，对 IIS 的请求必须在查询字符串或 Cookie 中包含有效的.NET Passport 凭据，提供了单一登录安全性，为用户提供对 Internet 上各种服务的访问权限。

基本身份验证：用户凭据以明文形式在网络中发送。这种形式提供的安全级别很低，因为几乎所有协议分析程序都能读取密码。所以答案是 C。

**参考答案**

（44）C

**试题（45）**

某局域网采用 SNMP 进行网络管理，所有被管设备在 15 分钟内轮询一次，网络没有明显拥塞，单个轮询时间为 0.4s，则该管理站最多可支持__（45）__个设备。

（45）A．18000　　B．3600　　C．2250　　D．90000

**试题（45）分析**

本题考查 SNMP 的基础知识。

SNMP 在进行网络管理时采用轮询机制，通常轮询频率与网络的规模和代理的多少有关。而网络管理性能还取决于管理站的处理速度、子网数据速率、网络拥塞程度等众多的因素。管理站轮询一般只是采用 get 请求/响应这种简单形式，而管理站主要操作用来轮询，测算管理站最多可支持设备采用如下不等式：

$$N \leqq T/\Delta$$

其中，$N$=被轮询的代理数；

$T$=轮询间隔；

$\Delta$=单个轮询需要的时间。

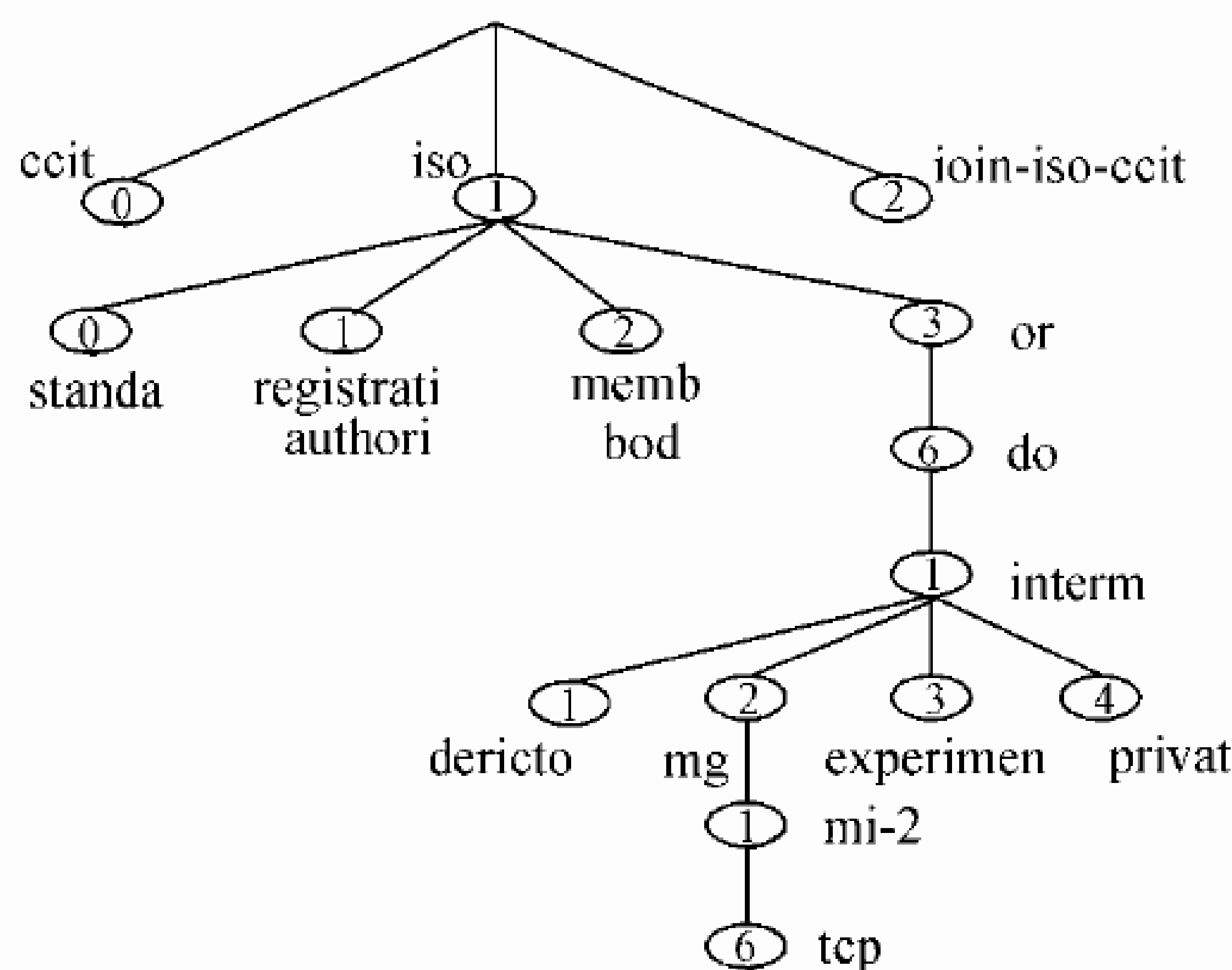
根据题目描述　$N \leqq T/\Delta=15\times60/0.4=2250$。

**参考答案**

（45）C

**试题（46）**

下图是被管理对象的树结构，其中 private 子树是为私有企业管理信息准备的，目前这个子树只有一个子结点 enterprises（1）。某私有企业向 Internet 编码机构申请到一个代码 920，该企业为它生产的路由器赋予的代码为 3，则该路由器的对象标识符是__（46）__。



（46）A．1.3.6.1.4.920.3　　B．3.920.4.1.6.3.1
C．1.3.6.1.4.1.920.3　　D．3.920.1.4.1.6.3.1

**试题（46）分析**

本题考查 SNMP 中管理对象树结构的基础知识。

SNMP 环境中的所有被管理对象组织成树型结构，如下图所示。这种层次树结构有 3 个作用：

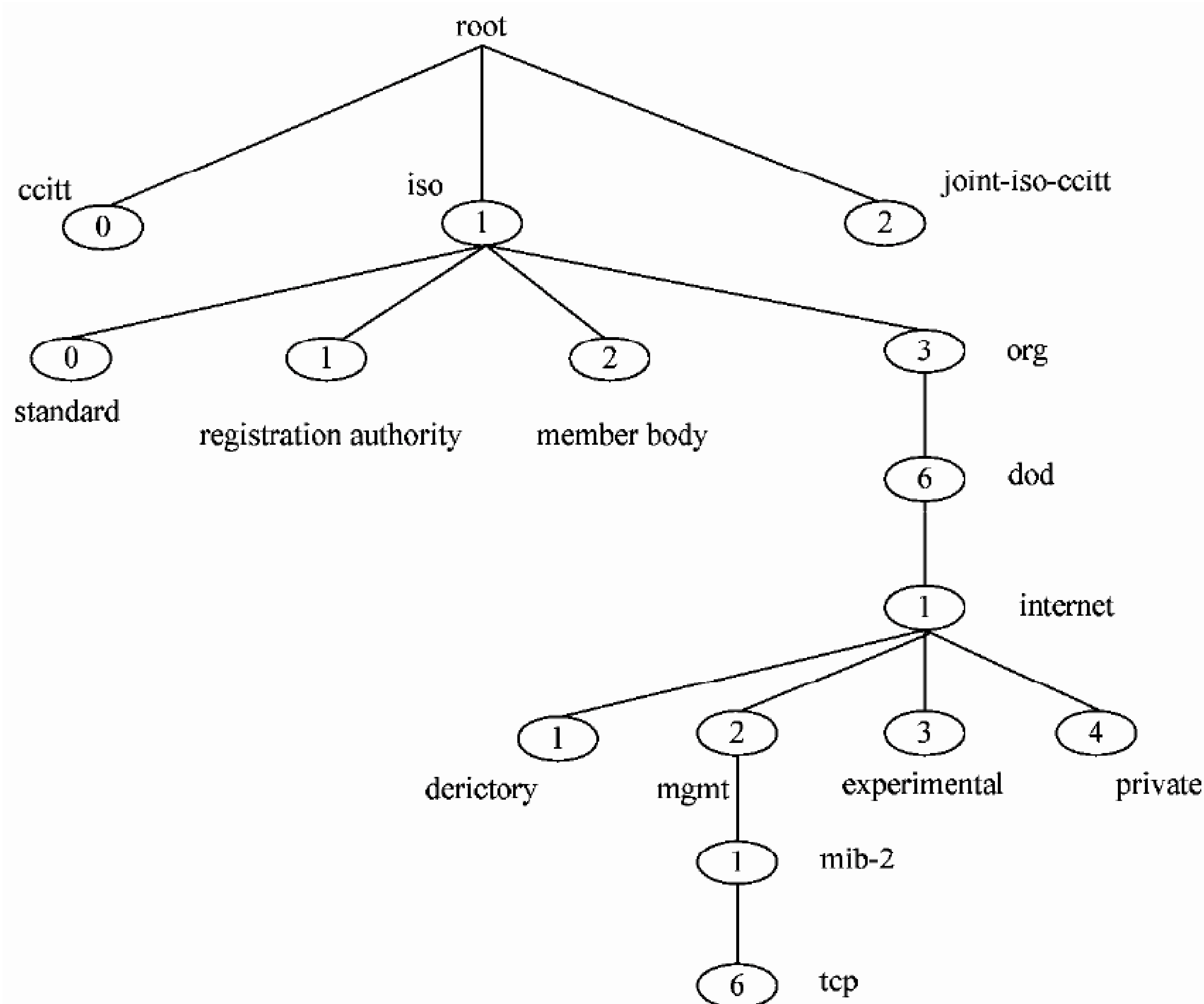



图　注册层次

① 表示管理和控制关系。从上图可知，上层的中间结点是某些组织机构的名字，说明这些机构负责它下面的子树的管理。有些中间结点虽然不是组织机构名，但已委托给某个组织机构代管，例如 org（3）由 ISO 代管，而 internet（1）由 IAB（Internet Architecture Board）代管等。树根没有名字，默认为抽象语法表示 ASN.1。

② 提供了结构化的信息组织技术。从上图可看出，下层的中间结点代表的子树是与每个网络资源或网络协议相关的信息集合。例如，有关 IP 协议的管理信息都放置在 ip(4) 子树中。这样，沿着树层次访问相关信息很方便。

③ 提供了对象命名机制。树中每个结点都有一个分层的编号。叶子结点代表实际的管理对象，从树根到树叶的编号串联起来，用圆点隔开，就形成了管理对象的全局标识。例如 internet 的标识符是 1.3.6.1，或者写为{iso(1) org(3) dod(6) 1}。

internet 下面的 4 个结点需要解释。directory 1 是 OSI 的目录服务（X.500）。mgmt 2 包括由 IAB 批准的所有管理对象，而 mib-2 是 mgmt 2 的第一个孩子结点。experimental 3 子树用来标识在互联网上实验的所有管理对象。最后，private 4 子树是为私有企业管理信息准备的，目前这个子树只有一个孩子结点 enterprises 1。

根据题目描述，某私有企业向 Internet 编码机构申请到一个代码 920，该企业为它生产的路由器赋予的代码为 3。这样，该路由器的对象标识符就是 1.3.6.1.4.1.920.3。

**参考答案**

（46）C

**试题（47）、（48）**

使用 Windows 提供的网络管理命令＿（47）＿可以查看本机的路由表，＿（48）＿可以修改本机的路由表。

（47）A．tracert　　B．arp　　C．ipconfig　　D．netstat

（48）A．ping　　B．route　　C．netsh　　D．nbtstat

**试题（47）、（48）分析**

本题考查网络管理命令的使用。

tracert 是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。

arp 命令用来显示和修改 arp 缓存中的值。

ipconfig 命令可用于显示当前的 TCP/IP 配置的设置值。

netstat 是 Windows 提供的网络管理命令，是一个监控 TCP/IP 网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。netstat 常用的参数如下：

- netstat-s：能够按照各个协议分别显示其统计数据。
- netstat-e：用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。
- netstat-r：可以显示关于路由表的信息，类似于后面所讲使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接。
- netstat-a：显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接。
- netstat-n：显示所有已建立的有效连接。

ping 命令是 Windows 系列自带的一个可执行命令。利用它可以检查网络是否能够连通。

route 用于显示本地 IP 路由表或修改本地路由表。

netsh 是 Windows 系统本身提供的功能强大的网络配置命令行工具。可以导入、导出配置脚本，还可以对 wins、route、ras 等网络服务的配置进行操作。

nbtstat 命令可以显示基于 TCP/IP 的 NetBIOS（NetBT）协议统计资料、本地计算

机和远程计算机的 NetBIOS 名称表和 NetBIOS 名称缓存。

**参考答案**

（47）D　（48）B

**试题（49）**

某局域网访问 Internet 速度很慢，经检测发现局域网内有大量的广播包，采用__（49）__方法不可能有效地解决该网络问题。

（49）A．在局域网内查杀 ARP 病毒和蠕虫病毒
B．检查局域网内交换机端口和主机网卡是否有故障
C．检查局域网内是否有环路出现
D．提高出口带宽速度

**试题（49）分析**

本题考查网络故障排查的基础知识。

局域网访问 Internet 速度很慢的原因可能是由于出口带宽速度不够或网络内部出现问题造成的。根据题目描述，发现局域网内有大量的广播包，造成这种情况的原因可能是有以下几种：

- ARP 病毒和蠕虫病毒攻击。
- 局域网内交换机端口和主机网卡出现故障。
- 局域网内出现环路。

**参考答案**

（49）D

**试题（50）**

下列 IP 地址中，属于私网地址的是__（50）__。

（50）A．100.1.32.7　　B．192.178.32.2
C．172.17.32.15　　D．172.35.32.244

**试题（50）分析**

有一些特殊的 IP 地址必须记住：

- 网络地址：主机地址全为 0 地址称为网络地址，例如 129.45.0.0 就是指一个 B 类网络地址。
- 广播地址：主机地址为全 1 的地址称为广播地址，例如 129.45.255.255 就是一个 B 类广播地址，网络 129.45.0.0 中的主机都可以接收这个数据报。
- 本地回路地址：网络地址 127 保留给诊断用，例如 127.0.0.1 用于回路测试。
- 本地网络地址：网络地址的第一个字节全为 0 时表示本地网络。
- 私网地址：这种地址不能在公网上出现，只能用在内部网络中，所有的路由器都不转发目标地址为私网地址的数据报。下面的地址都是私网地址：
  - 10.0.0.0～10.255.255.255　　1 个 A 类地址

- 172.16.0.0～172.31.255.255　　16 个 B 类地址
- 192.168.0.0～192.168.255.255　　256 个 C 类地址

**参考答案**

（50）C

**试题（51）**

网络 200.105.140.0/20 中可分配的主机地址数是__（51）__。

（51）A．1022　　B．2046　　C．4094　　D．8192

**试题（51）分析**

由于地址 200.105.140.0/20 中的子网掩码有 20 位，留给主机的地址只有 12 位，所以 $2^{12}-2=4094$。

**参考答案**

（51）C

**试题（52）**

下列地址中，属于 154.100.80.128/26 的可用主机地址是__（52）__。

（52）A．154.100.80.128　　B．154.100.80.190

C．154.100.80.192　　D．154.100.80.254

**试题（52）分析**

网络 154.100.80.128/26 中的主机地址都采用 154.100.80.10××××××形式，显然 154.100.80.192 和 154.100.80.254 都超出了地址范围，154.100.80.128 是子网地址，只有 154.100.80.190 属于规定的子网。

**参考答案**

（52）B

**试题（53）**

无类别域间路由（CIDR）技术有效地解决了路由缩放问题。使用 CIDR 技术把 4 个网络

C1：192.24.0.0/21

C2：192.24.16.0/20

C3：192.24.8.0/22

C4：192.24.34.0/23

汇聚成一条路由信息，得到的网络地址是__（53）__。

（53）A．192.24.0.0/13　　B．192.24.0.0/24

C．192.24.0.0/18　　D．192.24.8.0/20

**试题（53）分析**

网络 C1：192.24.0.0/21 的二进制表示为：**11000000 00011000 00000**000 00000000

网络 C2：192.24.16.0/20 的二进制表示为：**11000000 00011000 0001**0000 00000000

网络 C3：192.24.8.0/22 的二进制表示为：　**11000000 00011000 000010**00 00000000

网络 C4：192.24.34.0/23 的二进制表示为：　**11000000 00011000 0010001**0 00000000

地址 192.24.0.0/18 的二进制表示为：　**10101100 00011000 00**000000 00000000

所以 C 是正确答案。

**参考答案**

（53）C

**试题（54）、（55）**

网络 202.112.24.0/25 被划分为 4 个子网，由小到大分别命名为 C0、C1、C2 和 C3，则主机地址 202.112.24.25 应该属于　（54）　子网，主机地址 202.112.24.100 应该属于　（55）　子网。

（54）A．C0　　B．C1　　C．C2　　D．C3

（55）A．C0　　B．C1　　C．C2　　D．C3

**试题（54）、（55）分析**

网络 202.112.24.0/25 被划分成的 4 个子网是：

C0：202.112.24.0/27 的二进制表示为：　**11001010 01110000 00011000 000**00000

C1：202.112.24.32/27 的二进制表示为：　**11001010 01110000 00011000 001**00000

C2：202.112.24.64/27 的二进制表示为：　**11001010 01110000 00011000 010**00000

C3：202.112.24.96/27 的二进制表示为：　**11001010 01110000 00011000 011**00000

地址 202.112.24.25 的二进制表示为：　**11001010 01110000 00011000 000**11001

地址 202.112.24.100 的二进制表示为：　**11001010 01110000 00011000 011**00100

**参考答案**

（54）A　（55）D

**试题（56）、（57）**

交换机命令 show interfaces type 0/port_# switchport|trunk 用于显示中继连接的配置情况，下面是显示例子：

```
2950# show interface fastEthernet0/1 switchport
Name: fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
egotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
```

```
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
```

在这个例子中，端口 fa0/1 的链路模式被设置为__（56）__状态，默认的 VLAN 是__（57）__。

（56）A. Desirable　　B. No-Negotiate]
　　C. Auto negotiate　　D. trunk

（57）A. VLAN0　　B. VLAN1
　　C. VLAN2　　D. VLAN3

**试题（56）、（57）分析**

由 Administrative mode: trunk 和 Operational Mode: trunk 可看出，端口 fa0/1 的链路模式被设置为 trunk 状态，由 Trunking Native Mode VLAN: 1 (default)可看出，默认的 VLAN 是 VLAN1。

**参考答案**

（56）D　（57）B

**试题（58）**

按照 Cisco 公司的 VLAN 中继协议（VTP），当交换机处于__（58）__模式时可以改变 VLAN 配置，并把配置信息分发到管理域中的所有交换机。

（58）A. 客户机（Client）　　B. 传输（Transmission）
　　C. 服务器（Server）　　D. 透明（Transparent）

**试题（58）分析**

VLAN 中继协议（VLAN Trunking Protocol，VTP）是 Cisco 公司的专利协议。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为 3 种：

① 服务器模式（Server）：交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

② 客户机模式（Client）：在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

③ 透明模式（Transparent）：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

**参考答案**

（58）C

**试题（59）**

交换机命令 switch(config)# vtp pruning 的作用是＿（59）＿。

（59）A．指定交换机的工作模式　　B．启用 VTP 静态修剪

C．指定 VTP 域名　　D．启用 VTP 动态修剪

**试题（59）分析**

在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包，或者一个未知的单播数据包，交换机都会将其洪泛到所有与源 VLAN 端口相关的各个输出端口上，包括中继端口。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

虽然单个广播包尚不足以引起太大的问题，但是如果这是 PC-A 发出的 10Mb/s 的组播视频流，那么中继链路的吞吐率就会遇到严重的挑战。

为了解决这个问题，可以使用静态或动态修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪方式容易出错。

VTP 动态修剪允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

这样做的好处是显而易见的，如果以后在交换机 B 上添加了 VLAN 2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN 2，于是，两个交换机动态地把 VLAN 2 添加到它们之间的中继链路配置中，如下图所示。

VTP 动态修剪的缺点是它要求在 VTP 域中的所有交换机都必须配置成服务器。由于交换机在服务器模式下工作时可以改变 VLAN 配置，也可以接受 VLAN 配置的改变，所以当多个管理员在多个服务器上同时配置 VLAN 时将会出现灾难性的后果。

交换机命令 switch(config)# vtp pruning 的作用是启用 VTP 动态修剪。

**参考答案**

（59）D

**试题（60）**

IEEE 802.3 规定的最小帧长为 64 字节，这个帧长是指＿（60）＿。

（60）A．从前导字段到校验和的长度

B．从目标地址到校验和的长度

C．从帧起始符到校验和的长度

D．数据字段的长度

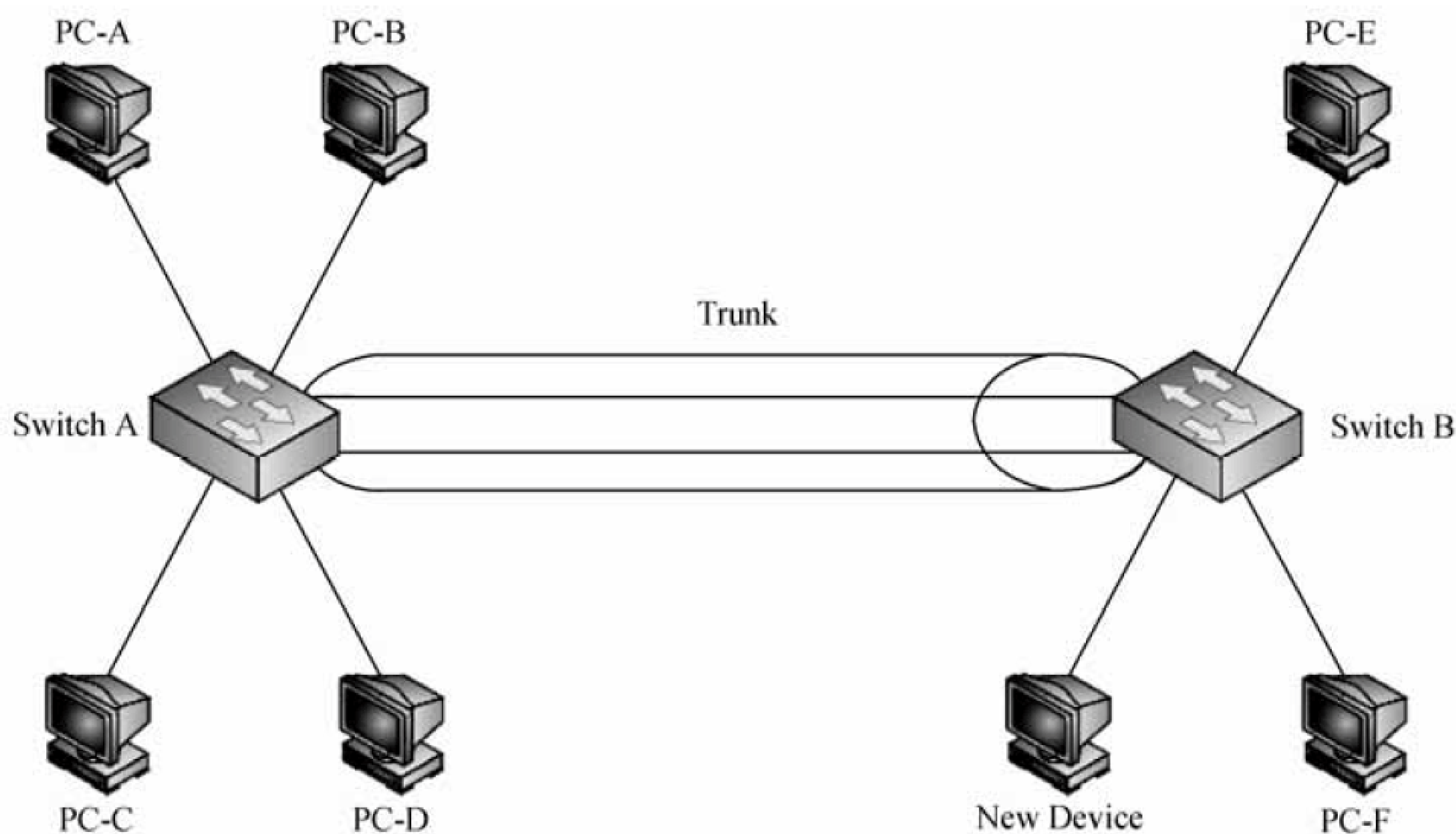



图 VTP 修剪

**试题（60）分析**

IEEE 802.3 规定的最小帧长为 64 字节，这个帧长是指从目标地址到校验和的长度，如下图所示。

| 字节数 | 6 | 6 | 2 | 0～1500 | 0～46 | 4 |
|---|---|---|---|---|---|---|
| | 目的地址 | 源地址 | 长度 | 数据 | 填充 | 校验和 |

图 802.3 的帧格式

**参考答案**

（60）B

**试题（61）**

千兆以太网标准 802.3z 定义了一种帧突发方式（frame bursting），这种方式是指<u>（61）</u>。

（61）A．一个站可以突然发送一个帧

B．一个站可以不经过竞争就启动发送过程

C．一个站可以连续发送多个帧

D．一个站可以随机地发送紧急数据

**试题（61）分析**

1998 年 6 月公布的 IEEE 802.3z 和 1999 年 6 月公布的 IEEE 802.3ab 已经成为千兆以太网的正式标准。它规定了四种传输介质，如下表所示。

**表　千兆以太网标准**

| 标　准 | 名　称 | 电　缆 | 最大段长 | 特　点 |
|---|---|---|---|---|
| IEEE 802.3z | 1000Base-SX | 光纤（短波 770～860nm） | 550m | 多模光纤（50，62.5μm） |
| | 1000Base-LX | 光纤（长波 1270～1355nm） | 5000m | 单模（10μm）或多模光纤（50，62.5μm） |
| | 1000Base-CX | 2 对 STP | 25m | 屏蔽双绞线，同一房间内的设备之间 |
| IEEE 802.3ab | 1000Base-T | 4 对 UTP | 100m | 5 类无屏蔽双绞线，8B/10B 编码 |

实现千兆数据速率需要采用新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外 802.3z 还定义了一种帧突发方式（frame bursting），使得一个站可以连续发送多个帧。最后物理层编码也采用了与 10Mb/s 不同的编码方法，即 4b/5b 或 8b/9b 编码法。

千兆以太网标准可用于已安装的综合布线基础之上，以保护用户的投资。

**参考答案**

（61）C

**试题（62）**

IEEE 802.11 标准定义的 Peer to Peer 网络是＿（62）＿。

（62）A．一种需要 AP 支持的无线网络

B．一种不需要有线网络和接入点支持的点对点网络

C．一种采用特殊协议的有线网络

D．一种高速骨干数据网络

**试题（62）分析**

IEEE 802.11 标准定义了两种无线网络拓扑结构，一种是基础设施网络（Infrastructure Networking），另一种是特殊网络（Ad Hoc Networking）。在基础设施网络中，无线终端通过接入点（Access Point，AP）访问骨干网设备，或者互相访问。接入点如同一个网桥，它负责在 802.11 和 802.3 MAC 之间进行转换。

Ad hoc 网络是一种点对点网络，不需要有线网络和接入点的支持，以无线网卡连接的终端设备之间可以直接通信。这种拓扑结构适合在固定或移动情况下快速部署网络。802.11 支持单跳的 Ad hoc 网络，当一个无线终端接入时首先寻找来自 AP 或其他终端的信标信号，如果找到了信标，则 AP 或其他终端就宣布新的终端加入了网络。如果没有检测到信标，该终端就自行宣布存在于网络之中。

**参考答案**

（62）B

**试题（63）**

IEEE 802.11g 标准支持的最高数据速率可达__（63）__Mb/s。

（63）A. 5　　B. 11　　C. 54　　D. 100

**试题（63）分析**

IEEE 公布的无线局域网正式标准如下表所示。

**表　IEEE 802.11 标准**

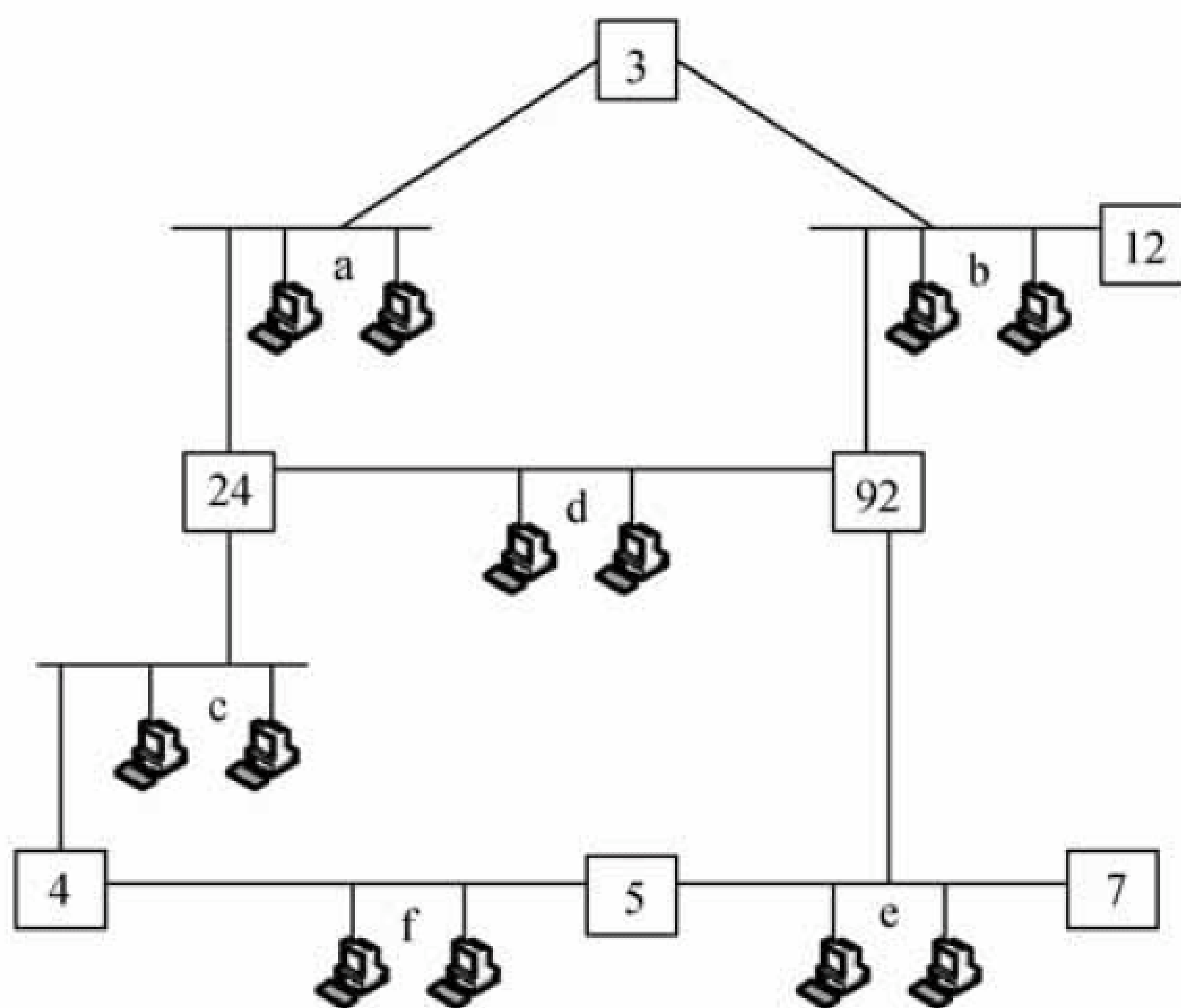
| 标准 | 时间 | 工 作 频 率 | 数 据 速 率 | 通 信 技 术 |
|---|---|---|---|---|
| 802.11 | 1997 | 2.4GHz ISM 频段 | 1Mb/s，2Mb/s | FHSS 或 DSSS |
| 802.11b | 1998 | 2.4GHz ISM 频段 | 最高 11Mb/s，可降低为 5.5Mb/s、2Mb/s、1Mb/s | DSSS |
| 802.11a | 1999 | 5GHz UNII 频段 | 物理层速率达 54Mb/s | OFDM |
| 802.11g | 2003 | 2.4GHz ISM 频段 | 强制速度 6Mb/s、12Mb/s 和 24 Mb/s | OFDM |

**参考答案**

（63）C

**试题（64）、（65）**

下图表示一个局域网的互连拓扑，方框中的数字是网桥 ID，用字母来区分不同的网段。按照 IEEE 802.1d 协议， ID 为__（64）__的网桥被选为根网桥，如果所有网段的传输费用为 1，则 ID 为 92 的网桥连接网段__（65）__的端口为根端口。




（64）A. 3　　B. 7　　C. 92　　D. 12

（65）A. a　　B. b　　C. d　　D. e

**试题（64）、（65）分析**

按照 IEEE 802.1d 协议定义的生成树算法，每个网桥有唯一的 MAC 地址和唯一的优

先级，地址和优先级构成网桥的标识符 ID，ID 最小的网桥被选举为根网桥。其他网桥的连接根网桥的费用最小的端口成为根端口。

**参考答案**

（64）A　（65）B

**试题（66）、（67）**

建筑物综合布线系统中的干线子系统是__（66）__，水平子系统是__（67）__。

（66）A．各个楼层接线间配线架到工作区信息插座之间所安装的线缆
B．由终端到信息插座之间的连线系统
C．各楼层设备之间的互连系统
D．连接各个建筑物的通信系统

（67）A．各个楼层接线间配线架到工作区信息插座之间所安装的线缆
B．由终端到信息插座之间的连线系统
C．各楼层设备之间的互连系统
D．连接各个建筑物的通信系统

**试题（66）、（67）分析**

结构化布线系统分为 6 个子系统：

① 工作区子系统（Work Location）：是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器以及传感器等多种终端设备。

② 水平子系统（Horizontal）：各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平子系统的作用是将干线子系统线路延伸到用户工作区。

③ 管理子系统（Administration）：管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆（跳线）互连，通过跳线的调整，可以对工作区的信息插座和交换机端口之间进行连接切换。

④ 干线子系统（Backbone）：干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头接于设备间的主配线架上，另一头接在楼层接线间的管理配线架上。

⑤ 设备间子系统（Equipment）：建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX，网络设备和监控设备等）之间的连接。

⑥ 建筑群子系统（Campus）：建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。大楼之间的布线方法有 3 种。一种是地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各种规定，安装时至少应预留 1～2 个备用管孔，以备

扩充之用。第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志。最后是架空明线，这种方法需要经常维护。

**参考答案**

（66）C　（67）A

**试题（68）**

假设生产管理网络系统采用 B/S 工作方式，经常上网的用户数为 150 个，每用户每分钟产生 8 个事务处理任务，平均事务量大小为 0.05MB，则这个系统需要的信息传输速率为__（68）__。

（68）A．4 Mb/s　　B．6 Mb/s

C．8 Mb/s　　D．12 Mb/s

**试题（68）分析**

可以根据下面的公式计算出应用需要的传输信息速率：

总信息传输速率＝平均事务量大小×每字节位数×每个会话事务数×平均用户数／平均会话时长

根据这个公式，结算结果为：0.05×8×8×150／60=8Mb/s。

**参考答案**

（68）C

**试题（69）、（70）**

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，每个阶段都要产生相应的文档。以下选项中，__（69）__属于逻辑网络设计文档，__（70）__属于物理网络设计文档。

（69）A．网络 IP 地址分配方案　　B．设备列表清单

C．集中访谈的信息资料　　D．网络内部的通信流量分布

（70）A．网络 IP 地址分配方案　　B．设备列表清单

C．集中访谈的信息资料　　D．网络内部的通信流量分布

**试题（69）、（70）分析**

一个网络系统从构思开始，到最后被淘汰的过程称为网络生命周期。一般来说，网络生命周期应包括网络系统的构思和计划、分析和设计、运行和维护的全过程。网络系统的生命周期与软件工程中的软件生命周期类似，首先它是一个循环迭代的过程，每次循环迭代的动力都来自于网络应用需求的变更。其次，每次循环过程中，都存在需求分析、规划设计、实施调试和运营维护等多个阶段。一般来说，网络规模越大，则可能经历的循环周期也越长。

每一个迭代周期都是网络重构的过程，不同的网络设计方法，对迭代周期的划分方式是不同的，拥有不同的网络文档模板，但是实施后的效果都满足了用户的网络需求。常见的迭代周期构成可分为五个阶段：需求规范、通信规范、逻辑网络设计、物理网络

设计、实施阶段。

在 5 个阶段中，每个阶段都是一个工作环节，每个环节完毕后才能进入到下一个环节，类似于软件工程中的“瀑布模型”，形成了特定的工作流程。按照这种流程构建网络，在下一个阶段开始之前，前一阶段的工作已经完成，一般情况下，不允许返回到前面的阶段。

集中访谈和收集信息资料属于需求分析阶段，网络内部通信流量分析属于通信规范阶段，网络 IP 地址分配方案的制定属于逻辑网络设计阶段，建立设备列表属于物理网络设计阶段。

**参考答案**

（69）A　（70）B

**试题（71）～（75）**

Although a given waveform may contain frequencies over a very broad range, as a practical matter any transmission system will be able to accommodate only a limited band of __(71)__. This, in turn, limits the data rate that can be carried on the transmission __(72)__. A square wave has an infinite number of frequency components and hence an infinite __(73)__. However, the peak amplitude of the *k*th frequency component, $k_f$, is only 1/*k*, so most of the __(74)__ in this waveform is in the first few frequency components. In general, any digital waveform will have __(75)__ bandwidth. If we attempt to transmit this waveform as a signal over any medium, the transmission system will limit the bandwidth that can be transmitteD.

（71）A. frequencies　B. connections　C. diagrams　D. resources
（72）A. procedure　B. function　C. route　D. medium
（73）A. source　B. bandwidth　C. energy　D. cost
（74）A. frequency　B. energy　C. amplitude　D. phase
（75）A. small　B. limited　C. infinite　D. finite

**参考译文**

虽然一个给定的波形包含了很宽的频率范围，但是任何实际的传输系统只能够通过有限的频带。这样，就限制了传输介质可以承载的数据速率。一个方波包含了无限多的频率成分，因而也具有无限的带宽。然而，第 *k* 个频率成分的峰值幅度 $k_f$ 只是 *1/k*，所以波形的大部分能量只是包含在前面的少数频率成分中。一般来说，任何数字波形都有无限带宽。如果我们试图在某种介质上传输这种波形信号，则传输系统实际上会限制可以发送的带宽。

**参考答案**

（71）A　（72）D　（73）B　（74）B　（75）C

# 第 6 章　2010 上半年网络工程师下午试题分析与解答

**试题一（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某校园网拓扑结构如图 1-1 所示。

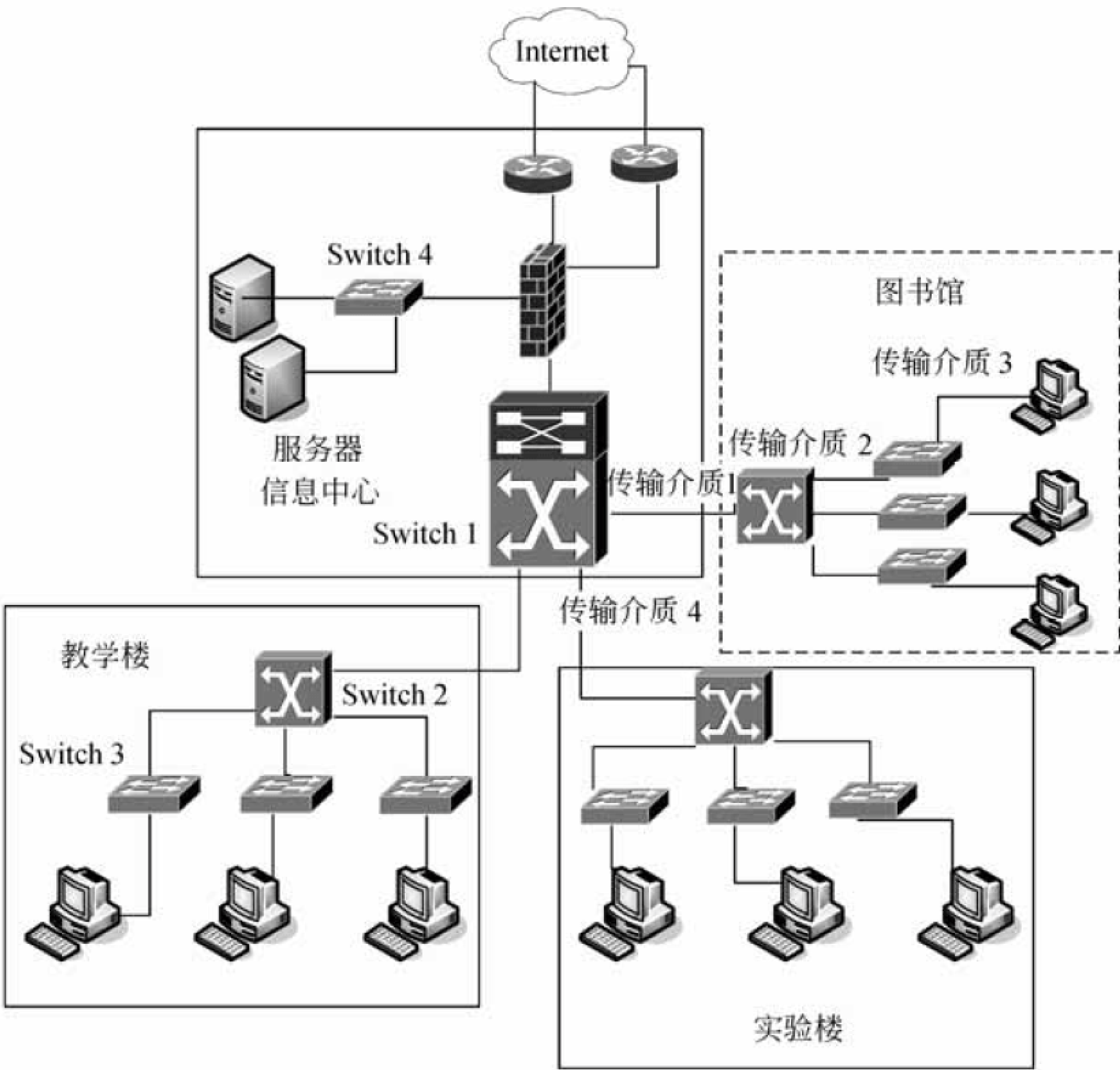



图 1-1

该网络中的部分需求如下：

1．信息中心距图书馆 2 千米，距教学楼 300 米，距实验楼 200 米。

2．图书馆的汇聚交换机置于图书馆主机房内，楼层设备间共 2 个，分别位于二层和四层，距图书馆主机房距离均大于 200 米，其中，二层设备间负责一、二层的计算机接入，四层设备间负责三、四、五层的计算机接入，各层信息点数如表 1-1 所示。

**表 1-1**

| 楼　层 | 信 息 点 数 |
|---|---|
| 1 | 24 |
| 2 | 24 |
| 3 | 19 |
| 4 | 21 |
| 5 | 36 |

3．所有计算机采用静态 IP 地址。

4．学校网络要求千兆干线，百兆到桌面。

5．信息中心有两条百兆出口线路，在防火墙上根据外网 IP 设置出口策略，分别从两个出口访问 Internet。

6．信息中心共有多台服务器，通过交换机接入防火墙。

7．信息中心提供的信息服务包括 Web、FTP、数据库、流媒体等，数据流量较大，要求千兆接入。

**【问题 1】（4 分）**

根据网络的需求和拓扑图，在满足网络功能的前提下，本着最节约成本的布线方式，传输介质 1 应采用＿（1）＿，传输介质 2 应采用＿（2）＿，传输介质 3 应采用＿（3）＿，传输介质 4 应采用＿（4）＿。

（1）～（4）备选答案：

A．单模光纤　　B．多模光纤　　C．基带同轴电缆

D．宽带同轴电缆　　E．1 类双绞线　　F．5 类双绞线

**【问题 2】（6 分）**

学校根据网络需求选择了四种类型的交换机，其基本参数如表 1-2 所示。

**表 1-2**

| 交换机类型 | 参　数 |
|---|---|
| A | 12 个固定千兆 RJ45 接口，背板带宽=24G，包转发率=18Mpps |
| B | 24 个千兆 SFP，背板带宽=192G，包转发率=150Mpps |
| C | 模块化交换机，背板带宽=1.8T，包转发率=300Mpps，业务插槽数量=8，支持电源冗余 |
| D | 24 个固定百兆 RJ45 接口，1 个 GBIC 插槽，包转发率=7.6 Mpps |

根据网络需求、拓扑图和交换机参数类型，在图 1-1 中，Switch 1 应采用＿（5）＿类型交换机，Switch 2 应采用＿（6）＿类型交换机，Switch 3 应采用＿（7）＿类型交换机，Switch 4 应采用＿（8）＿类型交换机。

根据需求描述和所选交换机类型，图书馆二层设备间最少需要交换机___(9)___台，图书馆四层设备间最少需要交换机___(10)___台。

**【问题 3】（3 分）**

该网络采用核心层、汇聚层、接入层的三层架构。根据层次化网络设计的原则，数据包过滤、协议转换应在___(11)___层完成；___(12)___层提供高速骨干线路；MAC 层过滤和 IP 地址绑定在___(13)___层完成。

**【问题 4】（2 分）**

根据该网络的需求，防火墙至少需要___(14)___个百兆接口和___(15)___个千兆接口。

**试题一分析**

本题考查网络规划和网络设备选型的知识。

**【问题 1】**

本问题考查网络传输介质的选用知识。

根据网络的需求和拓扑图，传输介质 1 连接信息中心核心交换机和图书馆汇聚交换机，两地之间距离 2 千米，且网络要求千兆干线，所以应该采用单模光纤。传输介质 2 连接图书馆汇聚交换机和图书馆接入交换机，两地之间距离大于 200 米，所以应该采用多模光纤。传输介质 3 连接图书馆接入交换机和接入 PC，网络要求百兆到桌面，根据拓扑结构，在选项中应选择 5 类双绞线。传输介质 4 连接信息中心核心交换机和实验楼汇聚交换机，两地之间距离 200 米，所以应该采用多模光纤。

**【问题 2】**

本问题考查交换机设备选型问题。

根据交换机参数类型判断，A 类交换机是 12 口千兆 RJ45 端口交换机，适合做千兆设备接入、B 类交换机是 24 口光纤接口交换机，背板速度较高，可以作为小型汇聚交换机、C 类交换机背板带宽和包转发率高，且为模块化设计，一般用于核心交换机使用，D 类交换机是标准百兆的接入交换机。

根据网络需求、拓扑图和交换机参数类型判断，在图 1-1 中，Switch 1 是核心交换机，所以应采用 A 类型交换机（核心交换机），Switch 2 是教学楼汇聚交换机，应采用 B 类型交换机（汇聚交换机），Switch 3 是教学楼接入交换机，应采用 C 类型交换机（百兆接入交换机），Switch 4 是信息中心服务器接入交换机，因为信息中心数据流量较大，要求千兆接入，应采用 A 类型交换机（千兆接入交换机）。

根据需求描述，图书馆二层设备间负责一、二层的计算机接入（共 48 个接入点），四层设备间负责三、四、五层的计算机接入（共 76 个接入点）。根据拓扑结构，图书馆接入交换机应采用 GBIC 插槽，使用多模光纤上联到图书馆汇聚交换机，再根据所选交换机类型参数（24 个固定百兆 RJ45 接口，1 个 GBIC 插槽）判断，图书馆二层设备间最少需要接入交换机两台，图书馆四层设备间最少需要接入交换机 4 台。

【问题 3】

本问题考查层次化网络中各分层的功能的基本概念。

层次化网络模型中一般将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用；核心层提供高速干线和不同区域的最优传送路径；汇聚层将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略，数据包过滤、协议转换都在汇聚层完成；接入层为局域网接入广域网或者终端用户访问网络提供接入，MAC 层过滤和 IP 地址绑定都在接入层完成。

【问题 4】

本问题考查防火墙设备接口的基本概念。

根据网络拓扑和题目需求描述可知，信息中心有两条百兆出口线路，在防火墙上根据外网 IP 设置出口策略，分别从两个出口访问 Internet，所以防火墙需要两个百兆接口。再根据需求描述可知，内部网络干线为千兆、服务器需要千兆接入，所以防火墙还需要两个千兆接口。

**参考答案**

【问题 1】

（1）A 或单模光纤

（2）B 或多模光纤

（3）F 或 5 类双绞线

（4）B 或多模光纤

【问题 2】

（5）C

（6）B

（7）D

（8）A

（9）2

（10）4

【问题 3】

（11）汇聚层

（12）核心层

（13）接入层

【问题 4】

（14）2

（15）2

**试题二（共 15 分）**

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

在 Linux 服务器中，inetd/xinetd 是 Linux 系统中一个重要服务。

【问题 1】（2 分）

下面选项中 （1） 是 xinetd 的功能。

（1）备选答案：

A．网络服务的守护进程　　B．定时任务的守护进程

C．负责配置网络接口　　D．负责启动网卡

【问题 2】（2 分）

默认情况下，xinetd 配置目录信息为：

drwxr-xr-x 2 root　root　4096 2009004-23 18:27 xinetd.d

则下列说法错误的是 （2） 。

（2）备选答案：

A．root 用户拥有可执行权限

B．除 root 用户外，其他用户不拥有执行权限

C．root 用户拥有可写权限

D．除 root 用户外，其他用户不拥有写权限

【问题 3】（4 分）

在 Linux 系统中，inetd 服务的默认配置文件为 （3） 。

（3）备选答案：

A．/etc/inet.conf　　B．/etc/inetd.config

C．/etc/inetd.conf　　D．/etc/inet.config

在 Linux 系统中，默认情况下，xinetd 所管理服务的配置文件存放在 （4） 。

（4）备选答案：

A．/etc/xinetd/　　B．/etc/xinetd.d/

C．/usr/etc/xinetd/　　D．/usr/etc/xinetd.d/

【问题 4】（4 分）

某 Linux 服务器上通过 xinetd 来对各种网络服务进行管理，该服务器上提供 ftp 服务，ftp 服务器程序文件为/usr/bin/ftpd，ftp 服务器的配置文件/etc/xinetd.d/ftp 内容如下所示，目前该服务器属于开启状态：

```
service ftp
       {
              socket_type           = stream
                protocol            = （5）
                wait                = no
                user                = root
                server              = （6）
                server_args        = -el
```

```
                disable            = no
        }
```

请完善该配置文件。

（5）备选答案：

A．TCP　　B．UDP　　C．IP　　D．HTTP

（6）备选答案：

A．/usr/bin/ftpd　　B．ftpd　　C．ftp　　D．/bin/ftpd

**【问题 5】（3 分）**

xinetd 可使用 only_from、no_access 以及 access_time 等参数对用户进行访问控制。若服务器上 ftp 服务的配置信息如下所示：

```
service ftp
{
......
only-from         = 192.168.3.0/24 172.16.0.0
no_access         = 172.16.{1,2}
access_times      = 07:00-21:00
......
}
```

则下列说法中错误的是＿（7）＿。

（7）备选答案：

A．允许 192.168.3.0/24 中的主机访问该 ftp 服务器

B．172.16.3.0/24 网络中的主机可以访问该 ftp 服务器

C．IP 地址为 172.16.×.× 的主机可以连接到此主机，但地址属于 172.16.1.×、172.16.2.×的则不能连接

D．ftp 服务器可以 24 小时提供服务

**试题二分析**

本题考查 Linux 下网络服务守护进程 inetd/xinetd 的相关概念。

**【问题 1】**

Xinetd 是一个守护程序，主要用于管理网络服务，因此本题选择 A。

**【问题 2】**

本问题考查 Linux 下文件权限的基础知识，从目录权限信息可知，应选择 B。

**【问题 3】**

本问题考查 inetd 和 xinetd 的默认配置文件存储位置，默认情况下 inetd 配置文件存储 etc/inetd.conf，xinetd 存储目录为/etc/xinetd.d/，因此（3）选择 C，（4）选择 B。

【问题 4】

本问题考查 xinetd 对网络服务的配置选项基本知识，从题干可知，该服务为 ftp 服务，服务器程序为/usr/bin/ftpd，由于 ftp 是基于 tcp 协议的，因此（5）应选择 A，（6）需要填写服务器程序路径，因此应选择 A。

【问题 5】

本问题考查 xinetd 对网络服务的访问权限基本知识，从配置中可以发现，ftp 服务不提供 24 小时访问，因此（7）应选择 D。

参考答案

【问题 1】

（1）A 或 网络服务的守护进程

【问题 2】

（2）B 或 除 root 用户外，其他用户不拥有执行权限

【问题 3】

（3）C 或 /etc/inetd.conf

（4）B 或 /etc/xinetd.d/

【问题 4】

（5）A 或 TCP

（6）A 或 /usr/bin/ftpd

【问题 5】

（7）D 或 ftp 服务器可以 24 小时提供服务

**试题三（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

终端服务可以使客户远程操作服务器，Windows Server 2003 中开启终端服务时需要分别安装终端服务的服务器端和客户端，图 3-1 为客户机 Host1 连接终端服务器 Server1 的网络拓扑示意图。

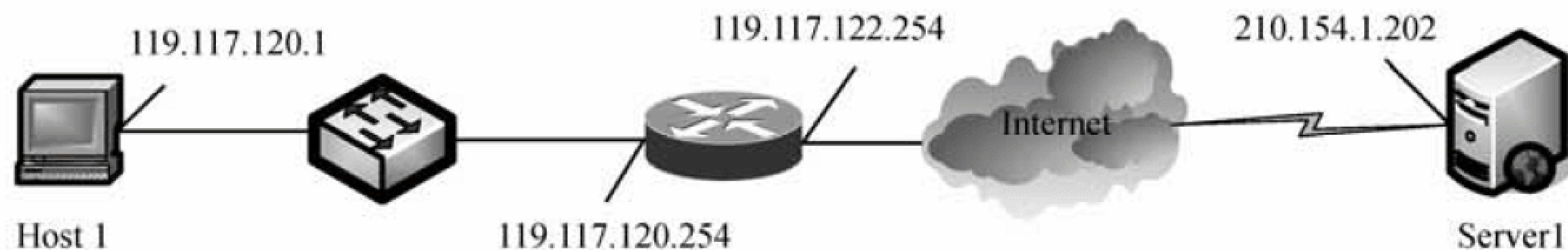



图 3-1

Host1 和 Server1 账户如表 3-1 所示。

**表 3-1**

| 账　户　名 | 主　　机 | 所　属　组 |
| --- | --- | --- |
| Admin1 | Host1 | Administrators |
| RDU1 | Host1 | Power Users |
| Admin2 | Server1 | Administrators |
| RDU2 | Server1 | Remote Desktop Users |

图 3-2 是 Server1“系统属性”的“远程”选项卡，图 3-3 是 Server1“RDP-Tcp 属性”的“环境”选项卡，图 3-4 为 Host1 采用终端服务登录 Server1 的用户登录界面。

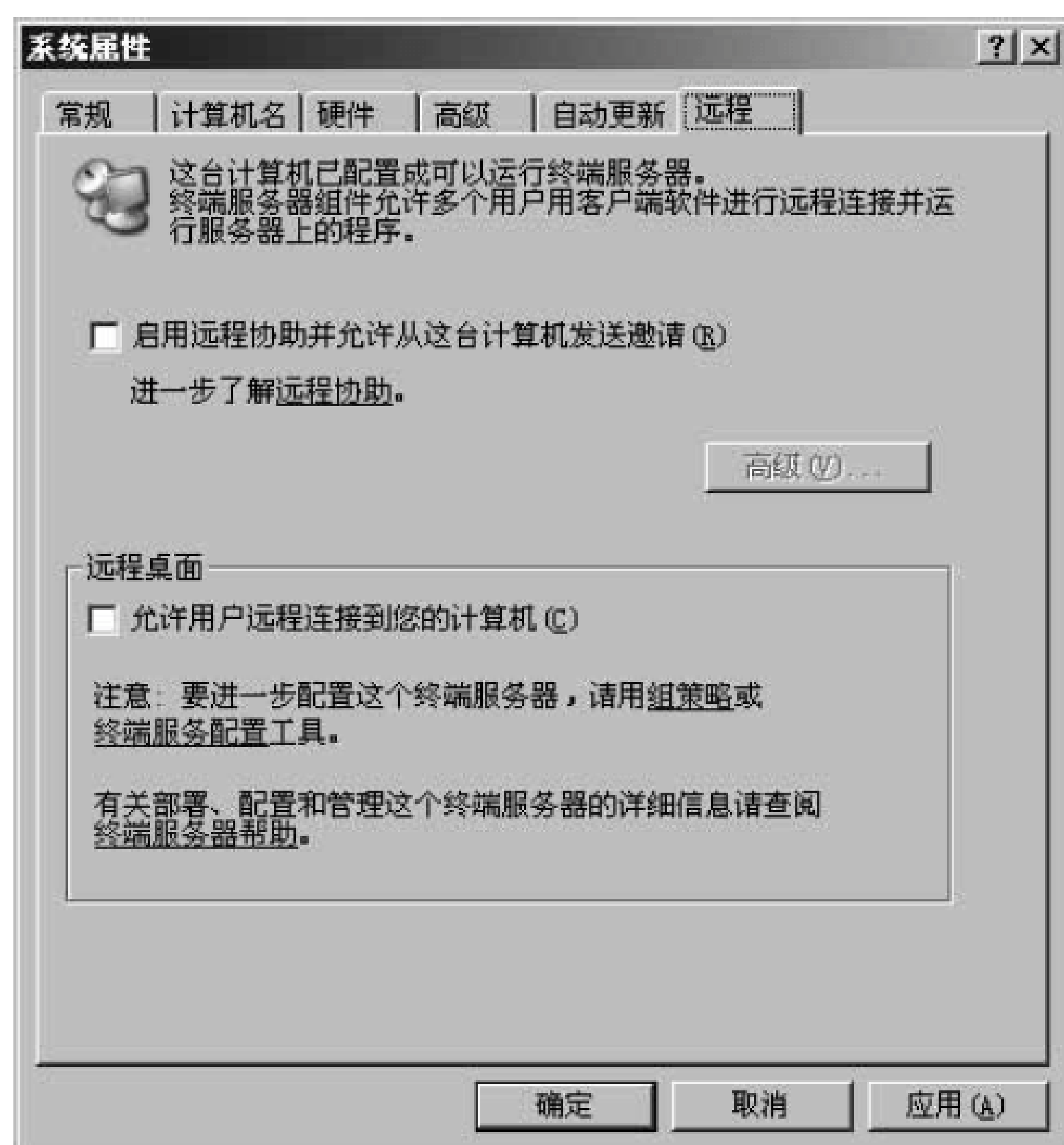



图 3-2

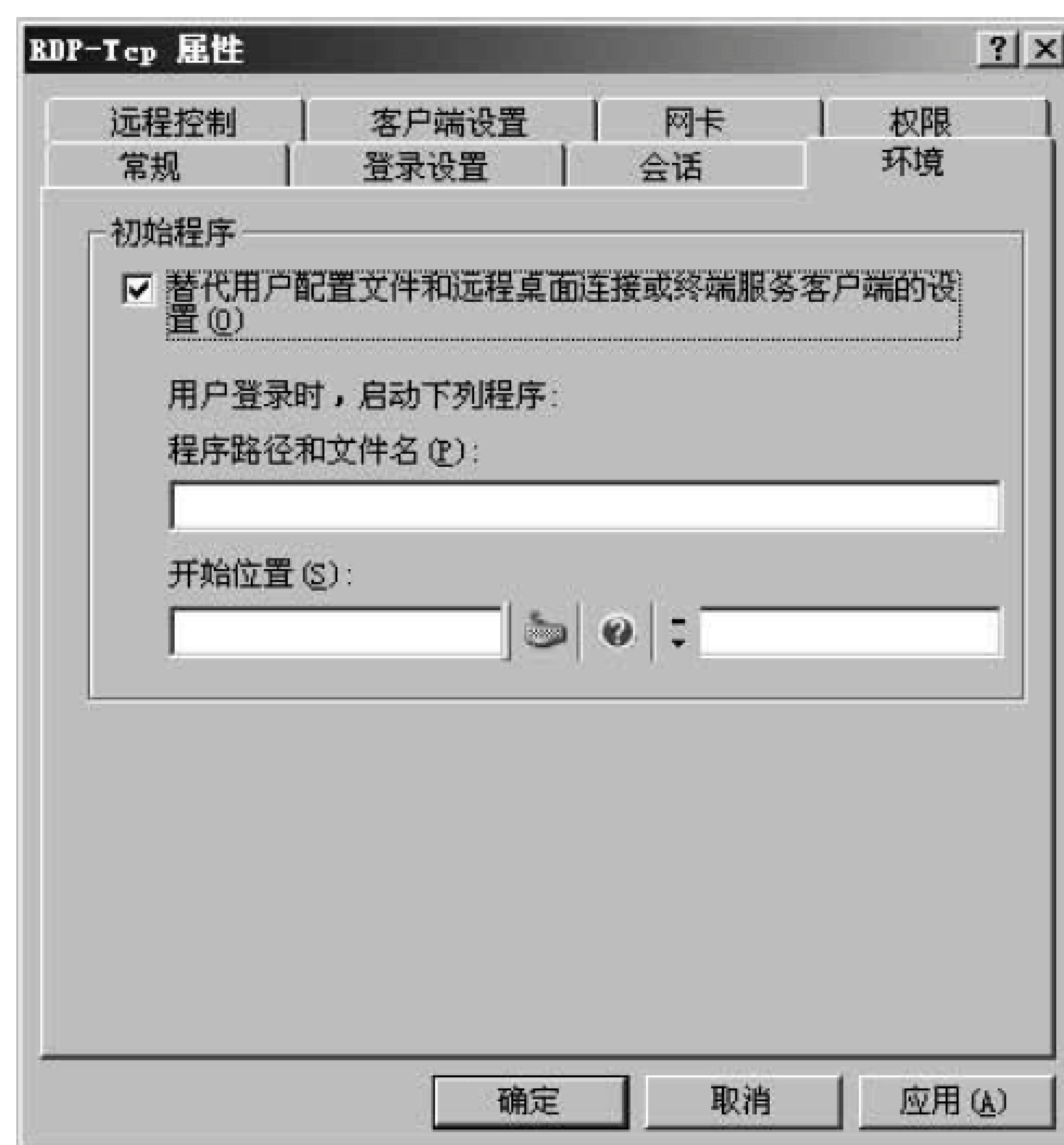



图 3-3

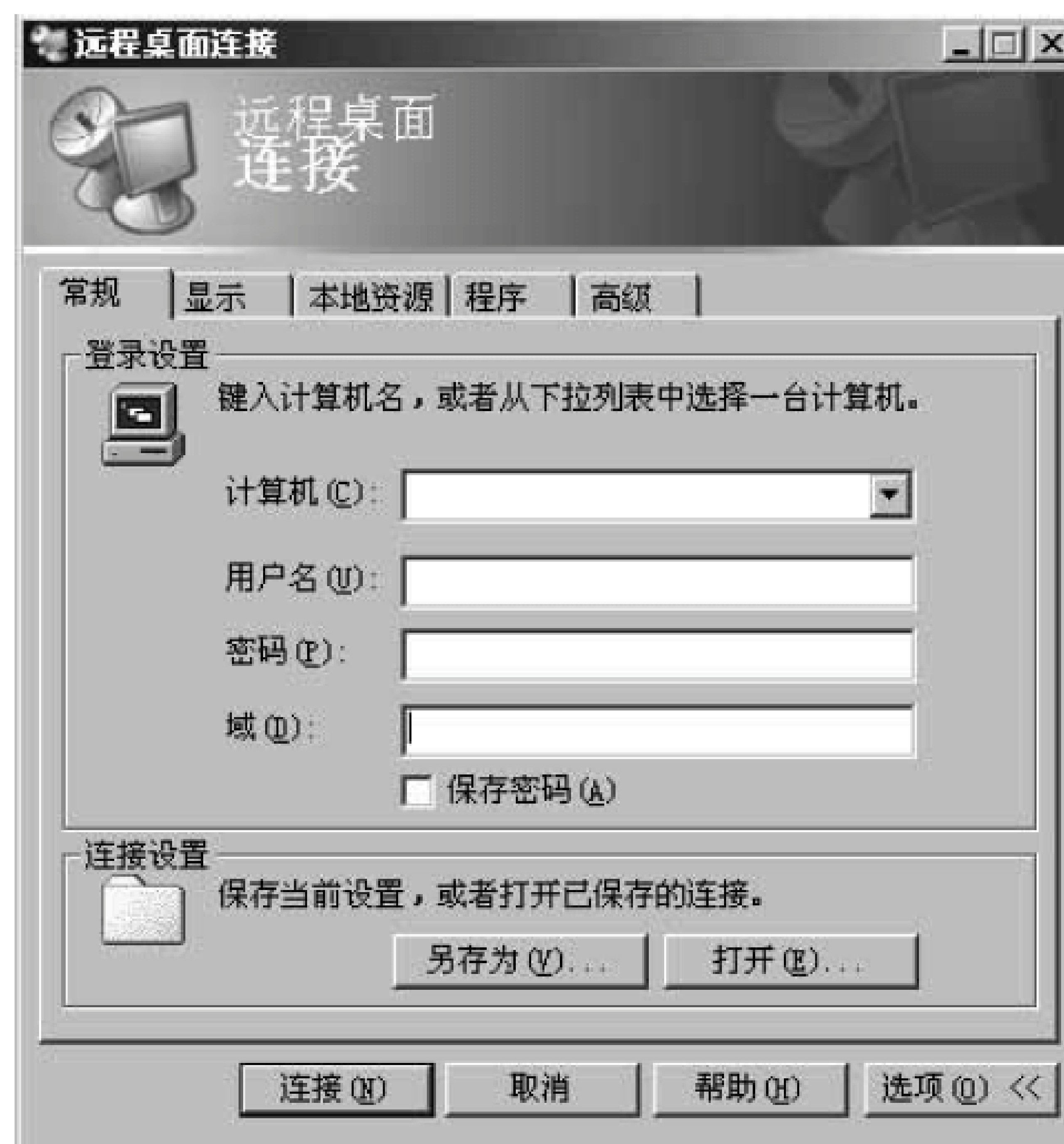



图 3-4

此外，在 Server1 中为了通过日志了解每个用户的行踪，把“D:\tom\note.bat”设置成用户的登录脚本，通过脚本中的配置来记录日志。

**【问题 1】（3 分）**

默认情况下，RDU2 对终端服务具有__（1）__和__（2）__权限。

（1）、（2）备选答案：

A．完全控制　　B．用户访问　　C．来宾访问　　D．特别权限

**【问题 2】（7 分）**

将 RDU2 设置为 Server1 的终端服务用户后，在 Host1 中登录 Server1 时，图 3-4 中“计算机”栏应填入__（3）__；“用户名”栏应填入__（4）__。

此时发现 Host1 不能远程登录终端服务器，可能原因是__（5）__。

**【问题 3】（2 分）**

在图 3-3“程序路径和文件名”栏中应输入__（6）__。

**【问题 4】（3 分）**

note.bat 脚本文件如下：

```
time /t >>note.log
netstat -n -p tcp | find ":3389">> note.log
start Explorer
```

第一行代码用于记录用户登录的时间，“time /t”的意思是返回系统时间，使用符号“>>”把这个时间记入“note.log”作为日志的时间字段。请解释下面命令的含义。

netstat -n -p tcp | find":3389">> note.log

**试题三分析**

本题考查 Windows Server 2003 中终端服务的配置与管理。

此类题目要求考生具备有实际的服务配置经历，通过掌握的基础知识，认真阅读题目场景来回答问题。

**【问题 1】**

默认情况下只有系统管理员组用户（Administrators）和系统组用户（SYSTEM）拥有访问和完全控制终端服务器的权限，另外远程桌面用户组（Remote Desktop Users）的成员只拥有访问权限而不具备完全控制权。

依据表 3-1，RDU2 属于远程桌面用户组，故其拥有用户访问和来宾访问的权限。

**【问题 2】**

客户机登录终端服务的服务器时，“计算机”栏应填入终端服务器的 IP 地址；“用户名”栏应填入终端服务用户，故（3）处应填入 210.154.1.202，（4）处应填入 RDU2。除此之外，要登录服务器，服务器中必须允许用户远程连接。

**【问题 3】**

（6）处应填入的是日志文件存放的目录，即 D:\tom\note.bat。

**【问题 4】**

netstat -n -p tcp | find":3389">> note.log 的目的是将远程访问主机的信息记录在日志文件 note.log 中，记录 3389 端口的 TCP 协议状态。

**参考答案** s

**【问题 1】**

（1）B 或 用户访问

（2）C 或 来宾访问

（（1）、（2）答案可互换）

**【问题 2】**

（3）210.154.1.202

（4）RDU2

（5）图 3-2 中没有勾选“允许用户远程连接到您的计算机”复选框

**【问题 3】**

（6）D:\tom\note.bat

**【问题 4】**

将通过 3389 端口访问主机的 TCP 协议状态信息写入 note.log 文件中，或将远程访问主机的信息记录在日志文件 note.log 中。

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

在 Windows Server 2003 系统中，用户分为本地用户和域用户，本地用户的安全策略用“本地安全策略”设置，域用户的安全策略通过活动目录管理。

**【问题 1】（2 分）**

在“本地安全设置”中启用了“密码必须符合复杂性要求”功能，如图 4-1 所示，则用户“ABC”可以采用的密码是__（1）__。

（1）备选答案：

A．ABC007　　B．deE#3　　C．Test123　　D．adsjfs

**【问题 2】（4 分）**

在“本地安全设置”中，用户账户锁定策略如图 4-2 所示，当 3 次无效登录后，用户账户被锁定的实际时间是__（2）__。如果“账户锁定时间”设置为 0，其含义为__（3）__。

（2）备选答案：

A．30 分钟　　B．10 分钟　　C．0 分钟　　D．永久锁定

（3）备选答案：

A．账户将一直被锁定，直到管理员明确解除对它的锁定

B．账户将被永久锁定，无法使用

C．账户锁定时间无效

D．账户锁定时间由锁定计数器复位时间决定

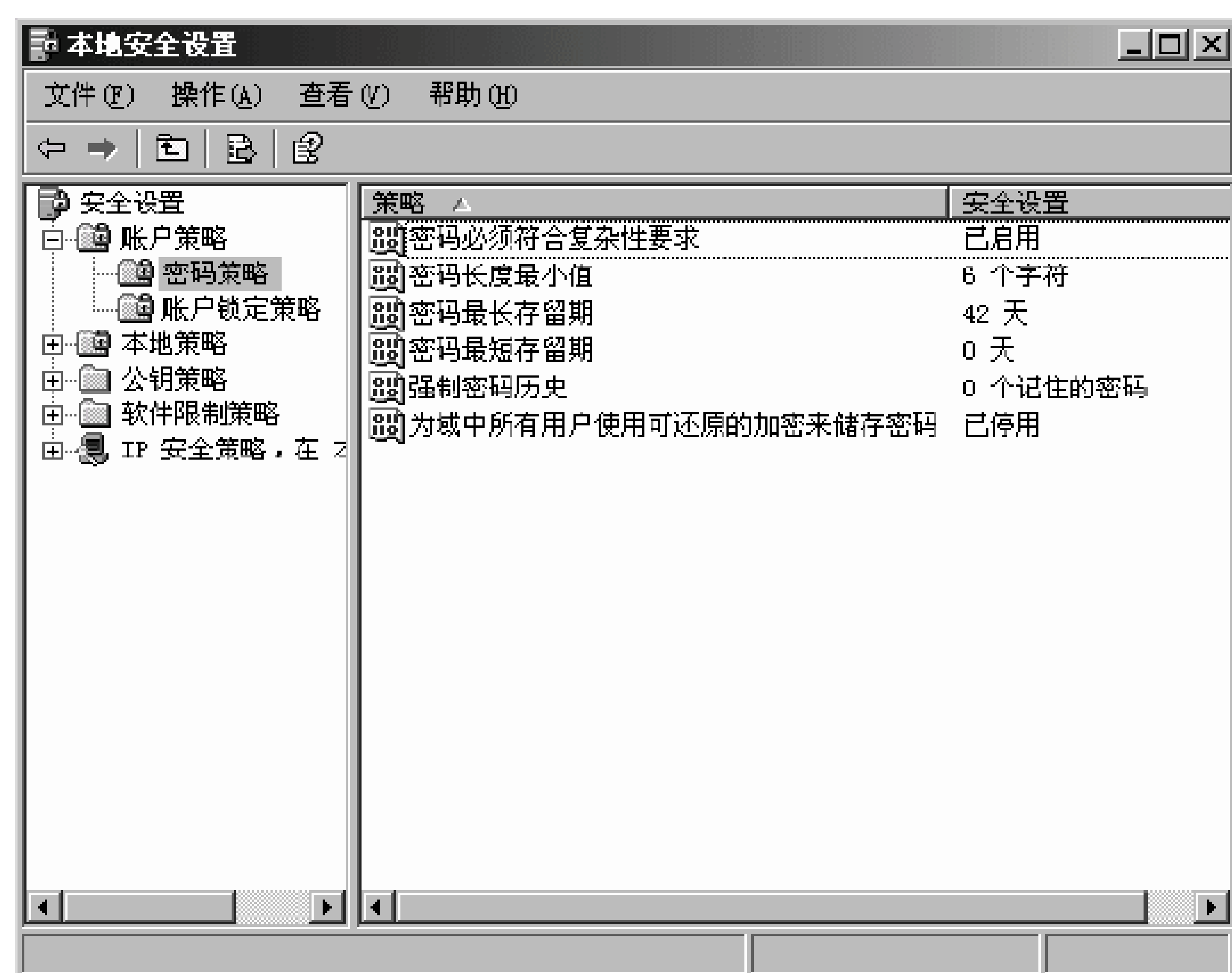



图 4-1




图 4-2

**【问题 3】（3 分）**

在 Windows Server 2003 中活动目录必须安装在__（4）__分区上，并且需要有__（5）__服务的支持。

（4）备选答案：

A．NTFS　　B．FAT32　　C．FAT16　　D．ext2

（5）备选答案：

A．Web　　B．DHCP　　C．IIS　　D．DNS

**【问题 4】（6 分）**

在 Windows Server 2003 的活动目录中，用户分为全局组（Global Groups）、域本地组（Domain Local Groups）和通用组（Universal Groups）。全局组的访问权限是__（6）__，域本地组的访问权限是__（7）__，通用组的访问权限是__（8）__。

（6）～（8）备选答案：

A．可以授予多个域中的访问权限

B．可以访问域林中的任何资源

C．只能访问本地域中的资源

**试题四分析**

本题考查 Windows Server 2003 中安全策略相关的配置。

**【问题 1】**

“本地安全设置”中启用了“密码必须符合复杂性要求”功能，启用该策略，则密码必须符合以下最低要求：

（1）不得明显包含用户账户名或用户全名的一部分。

（2）长度至少为六个字符。

（3）包含来自以下四个类别中的三个字符：

① 英文大写字母（从 A 到 Z）。

② 英文小写字母（从 a 到 z）。

③ 10 个基本数字（从 0 到 9）。

④ 非字母字符（例如，!、$、#、%）。

备选答案中选项 A 不满足上述要求 1，选项 B 不满足要求（2），选项 D 不满足要求（3），同时满足要求（1）、（2）和（3）的密码只有选项 C。

**【问题 2】**

在“本地安全设置”中，用户账户锁定策略中各项设置的含义如下：

（1）复位账户锁定计数器

此安全设置确定在某次登录尝试失败之后将登录尝试失败计数器重置为 0 次错误登录尝试之前需要的时间。

（2）账户锁定时间

此安全设置确定锁定账户在自动解锁之前保持锁定的分钟数。可用范围从 0 到 99 999 分钟。如果将账户锁定时间设置为 0，账户将一直被锁定直到管理员明确解除对它的锁定。

（3）账户锁定阈值

此安全设置确定导致用户账户被锁定的登录尝试失败的次数。在管理员重置锁定账户或账户锁定时间期满之前，无法使用该锁定账户。可以将登录尝试失败次数设置为介于 0 和 999 之间的值。如果将值设置为 0，则永远不会锁定账户。

从图 4-2 可知，用户 3 次登录失败后账户将会被锁定，实际锁定时间是 30 分钟，如果设置账户锁定时间为 0，账户将一直被锁定直到管理员明确解除对它的锁定。

**【问题 3】**

安装活动目录的必备条件包括一个 NTFS 磁盘分区和一个 DNS 服务器。

安装活动目录过程中，SYSVOL 文件夹必须存储在 NTFS 磁盘分区。SYSVOL 文件夹存储着与组策略等有关的数据。

活动目录与 DNS 是紧密集成的，活动目录中域的名称的解析需要 DNS 的支持。而域控制器也需要登记到 DNS 服务器内，以便其他计算机通过 DNS 服务器查找到这台域控制器。

**【问题 4】**

在 Windows Server 2003 的活动目录中，用户分为全局组（Global Groups）、域本地

组（Domain Local Groups）和通用组（Universal Groups）。

全局组成员来自于同一域的用户账户和全局组，可以访问域林中的任何资源。

域本地组成员来自林中任何域中的用户账户、全局组和通用组以及本域中的域本地组，只能访问本地域中的资源。

通用组成员来自林中任何域中的用户账户、全局组和其他的通用组，可以授予多个域中的访问权限。

**参考答案**

**【问题 1】**

（1）C

**【问题 2】**

（2）A

（3）A

**【问题 3】**

（4）A

（5）D

**【问题 4】**

（6）B

（7）C

（8）A

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位网络内部部署有 IPv4 主机和 IPv6 主机，该单位计划采用 ISATAP 隧道技术实现两类主机的通信，其网络拓扑结构如图 5-1 所示，路由器 R1、R2、R3 通过串口经 IPv4 网络连接，路由器 R1 连接 IPv4 网络，路由器 R3 连接 IPv6 网段。通过 ISATAP 隧道将 IPv6 的数据包封装到 IPv4 的数据包中，实现 PC1 和 PC2 的数据传输。

**【问题 1】（2 分）**

双栈主机使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。在 ISATAP 地址中，前 64 位是向 ISATAP 路由器发送请求得到的，后 64 位中由两部分构成，其中前 32 位是__（1）__，后 32 位是__（2）__。

（1）备选答案：

A．0:5EFE　　B．5EFE:0　　C．FFFF:FFFF　　D．0:0

（2）备选答案：

A．IPv4 广播地址　　B．IPv4 组播地址　　C．IPv4 单播地址

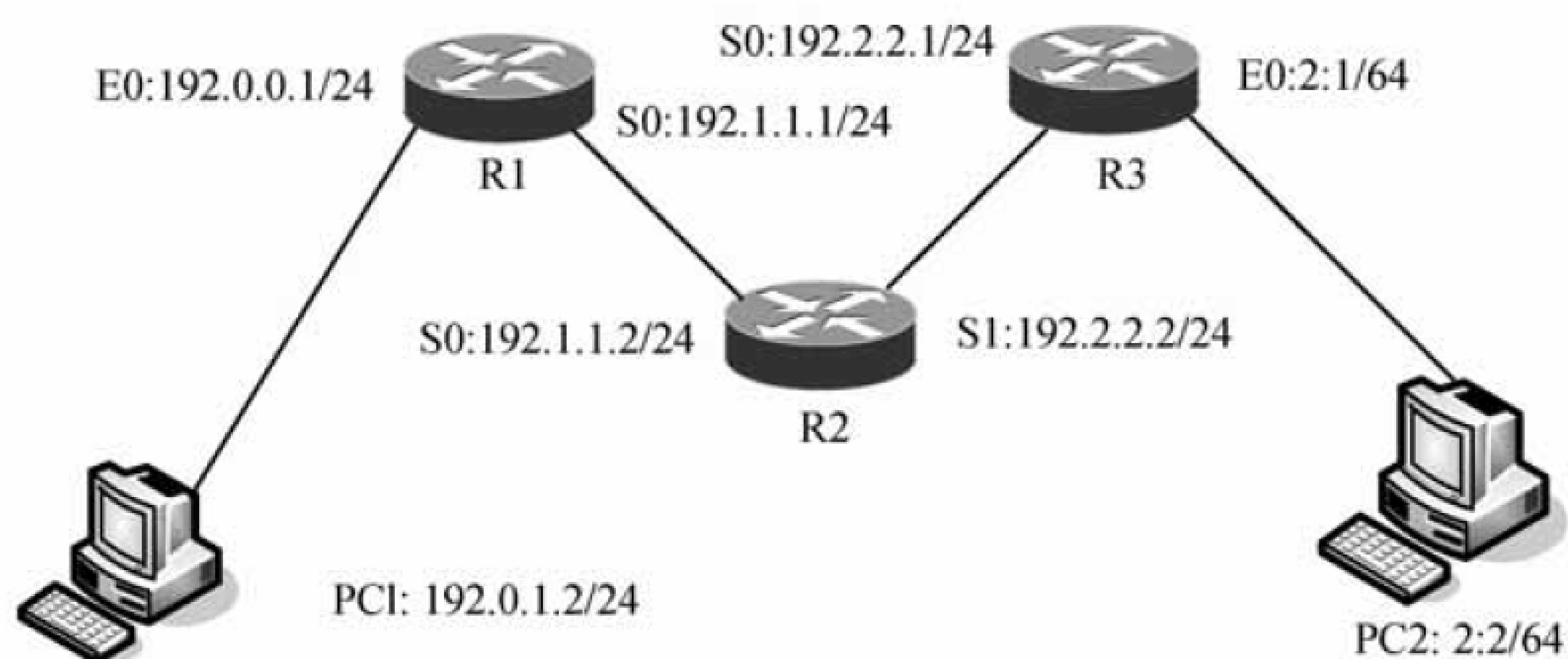



图 5-1

**【问题 2】**（6 分）

根据网络拓扑和需求说明，完成路由器 R1 的配置。

```
R1(config)# interface Serial 1/0
R1(config-if)# ip address  (3)  255.255.255.0         （设置串口地址）
R1(config-if)#no shutdown                              （开启串口）
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address  (4)  255.255.255.0           （设置以太口地址）
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#network 192.0.0.1  (5)  area 0
R1(config-router)#network 192.1.1.1  (6)  area 0
```

**【问题 3】**（6 分）

根据网络拓扑和需求说明，解释路由器 R3 的 ISATAP 隧道配置。

```
…
R3(config)#interface tunnel 0                            (7)
R3(config-if)# ipv6 address 2001:DA8:8000:3::/64 eui-64 为 tunnel 配置
IPv6 地址
R3(config-if)# no ipv6 nd suppress-ra              启用了隧道口的路由器广播
R3(config-if)#tunnel source s1/0                         (8)
R3(config-if)#tunnel mode ipv6ip isatap                  (9)
```

**【问题 4】**（1 分）

实现 ISATAP，需要在 PC1 进行配置，请完成下面的命令。

```
C:\> netsh interface ipv6 isatap set router  (10)
```

## 试题五分析

本题考查 ISATAP 隧道配置的知识。

**【问题 1】**

本问题考查 ISATAP 隧道的基本概念。

双栈主机使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的地址：ISATAP 地址。ISATAP 地址格式为：Prefix（64bit）:0:5EFE:IPv4ADDR，其中，0: 5EFE 是 IANA 规定的格式，IPv4ADDR 是单播 IPv4 地址，它嵌入到 IPv6 地址的低 32 位。ISATAP 地址的前 64 位是通过向 ISATAP 路由器发送请求得到的，如果需要和其他网络的 ISATAP 客户机或者 IPv6 网络通信，必须通过 ISATAP 路由器拿到全球单播地址前缀（2001:, 2002:, 3ffe:开头），通过路由器与其他 IPv6 主机和网络通信。

**【问题 2】**

本问题考查路由器接口地址及 OSPF 的基本配置操作。

根据拓扑结构图可知，路由器 R1 的 E0 口地址为：192.0.0.1/24；S0 口地址为：192.1.1.1/24，所以配置命令如下：

```
R1(config)# interface Serial 1/0
R1(config-if)# ip address 192.1.1.1 255.255.255.0    （设置串口地址）
R1(config-if)#no shutdown                            （开启串口）
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.0.0.1 255.255.255.0     （设置以太口地址）
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#network 192.0.0.1 0.0.0.255 area 0
R1(config-router)#network 192.1.1.1 0.0.0.255 area 0
```

**【问题 3】**

本问题考查 ISATAP 隧道基本配置操作。

```
R3(config)#interface tunnel 0                        启用 tunnel 0
R3(config-if)# ipv6 address 2001:DA8:8000:3::/64 eui-64 为 tunnel 配置
IPv6 地址
R3(config-if)# no ipv6 nd suppress-ra                启用了隧道口的路由器广播
R3(config-if)#tunnel source s1/0                     指定 tunnel 的源地址为 s0
R3(config-if)#tunnel mode ipv6ip isatap          tunnel 的模式为 ISATAP 隧道
```

**【问题 4】**

本问题考查使用 ISATAP 隧道时，PC 上的基本配置操作。

实现 ISATAP，需要在 PC 上进行配置，本题中 PC1 启用双栈，根据拓扑结构图，PC1 的 IPv6 路由应指定 R3 的 S0 口地址，所以配置操作如下：

C:\> netsh interface Ipv6 isatap set router 192.2.2.1

## 参考答案

**【问题 1】**

（1）A 或 0:5EFE

（2）C 或 IPv4 单播地址

**【问题 2】**

（3）192.1.1.1

（4）192.0.0.1

（5）0.0.0.255

（6）0.0.0.255

**【问题 3】**

（7）启用 tunnel 0

（8）指定 tunnel 的源地址为 s0

（9）tunnel 的模式为 ISATAP 隧道

**【问题 4】**

（10）192.2.2.1

# 第 7 章　2010 下半年网络工程师上午试题分析与解答

**试题（1）**

在输入输出控制方法中，采用 __（1）__ 可以使得设备与主存间的数据块传送无需CPU 干预。

（1）A. 程序控制输入输出　　B. 中断

C. DMA　　D. 总线控制

**试题（1）分析**

本题考查 CPU 中相关寄存器的基础知识。

计算机中主机与外设间进行数据传输的输入输出控制方法有程序控制方式、中断方式、DMA 等。

在程序控制方式下，由 CPU 执行程序控制数据的输入输出过程。

在中断方式下，外设准备好输入数据或接收数据时向 CPU 发出中断请求信号，CPU 若决定响应该请求，则暂停正在执行的任务，转而执行中断服务程序进行数据的输入输出处理，之后再回去执行原来被中断的任务。

在 DMA 方式下，CPU 只需向 DMA 控制器下达指令，让 DMA 控制器来处理数据的传送，数据传送完毕再把信息反馈给 CPU，这样就很大程度上减轻了 CPU 的负担，可以大大节省系统资源。

**参考答案**

（1）C

**试题（2）**

若某计算机采用 8 位整数补码表示数据，则运算 __（2）__ 将产生溢出。

（2）A. −127+1　　B. −127−1　　C. 127+1　　D. 127−1

**试题（2）分析**

本题考查计算机中的数据表示和运算的基础知识。

采用 8 位补码表示整型数据时，可表示的数据范围为−128～127，因此进行 127+1 的运算会产生溢出。

**参考答案**

（2）C

**试题（3）**

编写汇编语言程序时，下列寄存器中程序员可访问的是 __（3）__。

（3）A. 程序计数器（PC）　　B. 指令寄存器（IR）

C. 存储器数据寄存器（MDR）　　D. 存储器地址寄存器（MAR）

**试题（3）分析**

本题考查 CPU 中相关寄存器的基础知识。

指令寄存器（IR）用于暂存从内存取出的、正在运行的指令，这是由系统使用的寄存器，程序员不能访问。

存储器数据寄存器（MDR）和存储器地址寄存器（MAR）用于对内存单元访问时的数据和地址暂存，也是由系统使用的，程序员不能访问。

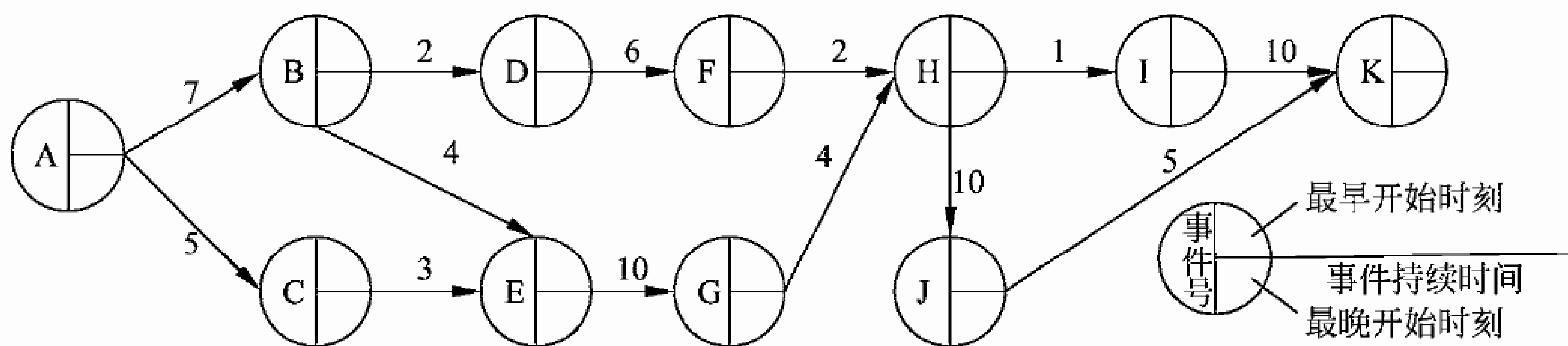
程序计数器（PC）用于存储指令的地址，CPU 根据该寄存器的内容从内存读取待执行的指令，程序员可以访问该寄存器。

**参考答案**

（3）A

**试题（4）、（5）**

使用 PERT 图进行进度安排，不能清晰地描述__（4）__，但可以给出哪些任务完成后才能开始另一些任务。下面的 PERT 图所示工程从 A 到 K 的关键路径是__（5）__（图中省略了任务的开始和结束时刻）。




（4）A. 每个任务从何时开始　　B. 每个任务到何时结束
　　C. 各任务之间的并行情况　　D. 各任务之间的依赖关系

（5）A. ABEGHIK　　B. ABEGHJK　　C. ACEGHIK　　D. ACEGHJK

**试题（4）、（5）分析**

本题考查软件项目管理的基础知识。

软件项目计划的一个重要内容是安排进度，常用的方法有 Gantt 图和 PERT 图。Gantt 图用水平条状图描述，它以日历为基准描述项目任务，可以清楚地表示任务的持续时间和任务之间的并行，但是不能清晰地描述各个任务之间的依赖关系。PERT 图是一种网络模型，描述一个项目的各任务之间的关系。可以明确表达任务之间的依赖关系，即哪些任务完成后才能开始另一些任务，以及如期完成整个工程的关键路径，但是不能清晰地描述各个任务之间的并行关系。

图中任务流 ABEGHIK 的持续时间是 36，ABEGHJK 的持续时间是 40，ACEGHIK 的持续时间是 33，ACEGHJK 的持续时间为 37。所以项目关键路径长度为 40。

**参考答案**

（4）C　　（5）B

**试题（6）**

某项目组拟开发一个大规模系统，且具备了相关领域及类似规模系统的开发经验。下列过程模型中，__（6）__最合适开发此项目。

（6）A. 原型模型　　B. 瀑布模型　　C. V 模型　　D. 螺旋模型

**试题（6）分析**

本题考查软件开发生命周期模型的基本知识。

常见的软件生存周期模型有瀑布模型、演化模型、螺旋模型、喷泉模型等。瀑布模型是将软件生存周期各个活动规定为依线性顺序连接的若干阶段的模型，适合于软件需求很明确的软件项目。V 模型是瀑布模型的一种演变模型，将测试和分析与设计关联进行，加强分析与设计的验证。原型模型是一种演化模型，通过快速构建可运行的原型系统，然后根据运行过程中获取的用户反馈进行改进。演化模型特别适用于对软件需求缺乏准确认识的情况。螺旋模型将瀑布模型和演化模型结合起来，加入了两种模型均忽略的风险分析。

本题中项目组具备了所开发系统的相关领域及类似规模系统的开发经验，即需求明确，瀑布模型最适合开发此项目。

**参考答案**

（6）B

**试题（7）**

软件复杂性度量的参数不包括__（7）__。

（7）A. 软件的规模　　B. 开发小组的规模
　　C. 软件的难度　　D. 软件的结构

**试题（7）分析**

软件复杂性度量是软件度量的一个重要分支。软件复杂性度量的参数有很多，主要包括：（1）规模，即指令数或者源程序行数；（2）难度，通常由程序中出现的操作数所决定的量来表示；结构，通常用与程序结构有关的度量来表示；（3）智能度，即算法的难易程度。

**参考答案**

（7）B

**试题（8）**

在操作系统文件管理中，通常采用__（8）__来组织和管理外存中的信息。

（8）A. 字处理程序　　B. 设备驱动程序
　　C. 文件目录　　D. 语言翻译程序

**试题（8）分析**

本题考查的是操作系统文件管理方面的基础知识。

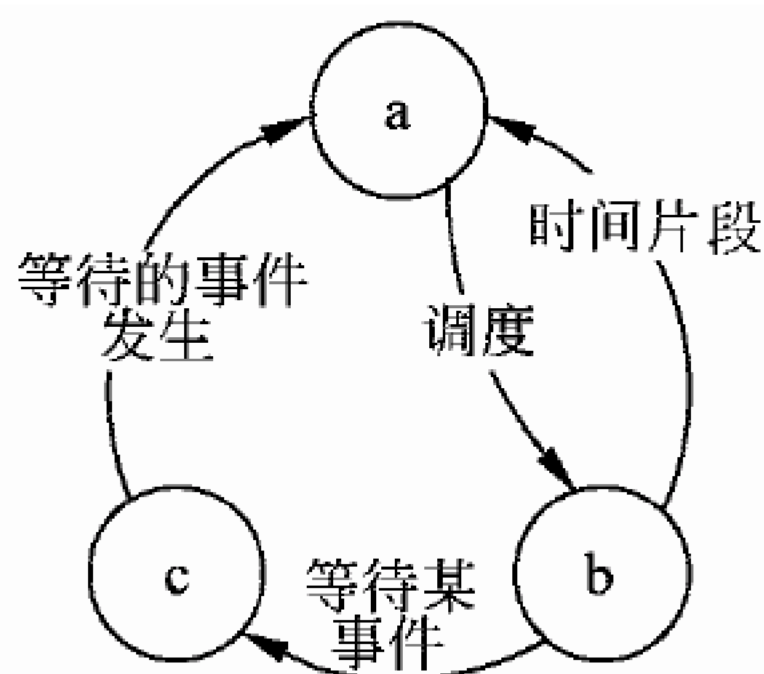
存放在磁盘空间上的各类文件必须进行编目，操作系统才能实现文件的管理，这与图书馆中的藏书需要编目录、一本书需要分章节是类似的。用户总是希望能“按名存取”文件中的信息。为此，文件系统必须为每一个文件建立目录项，即为每个文件设置用于描述和控制文件的数据结构，记载该文件的基本信息，如文件名、文件存放的位置、文件的物理结构等。这个数据结构称为文件控制块 FCB，文件控制块的有序集合称为文件目录。

**参考答案**

（8）C

**试题（9）**

假设系统中进程的三态模型如下图所示，图中的 a、b 和 c 的状态分别为__（9）__。




（9）A. 就绪、运行、阻塞　　B. 运行、阻塞、就绪
　　C. 就绪、阻塞、运行　　D. 阻塞、就绪、运行

**试题（9）分析**

本题考查操作系统进程管理方面的基础知识。

试题（9）的正确答案是 A。因为进程具有三种基本状态：运行态、就绪态和阻塞态。处于这三种状态的进程在一定条件下，其状态可以转换。当 CPU 空闲时，系统将根据某种调度算法选择处于就绪态的一个进程进入运行态；而当 CPU 的一个时间片用完时，当前处于运行态的进程就进入了就绪态；进程从运行到阻塞状态通常是由于进程释放 CPU，等待系统分配资源或等待某些事件的发生，如：执行了 P 操作，系统暂时不能满足其对某资源的请求，或等待用户的输入信息等；当进程正在等待的事件发生时，进程从阻塞到就绪状态，如 I/O 完成。

**参考答案**

（9）A

**试题（10）**

利用__（10）__可以对软件的技术信息、经营信息提供保护。

（10）A. 著作权　　B. 专利权　　C. 商业秘密权　　D. 商标权

**试题（10）分析**

本题考查知识产权方面的基础知识，涉及软件商业秘密权的相关概念。

著作权从软件作品性的角度保护其表现形式，源代码（程序）、目标代码（程序）、软件文档是计算机软件的基本表达方式（表现形式），受著作权保护；专利权从软件功能性的角度保护软件的思想内涵，即软件的技术构思、程序的逻辑和算法等的思想内涵，当计算机软件同硬件设备是一个整体，涉及计算机程序的发明专利，可以申请方法专利，取得专利权保护。商标权是为商业化的软件从商品、商誉的角度为软件提供保护，利用商标权可以禁止他人使用相同或者近似的商标、生产（制作）或销售假冒软件产品。商标权受保护的力度大于其他知识产权，对软件的侵权行为更容易受到行政查处。而商业秘密权是商业秘密的合法控制人采取了保密措施，依法对其经营信息和技术信息享有的专有使用权，我国《反不正当竞争法》中对商业秘密的定义为“不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息”。软件技术秘密是指软件中适用的技术情报、数据或知识等，包括程序、设计方法、技术方案、功能规划、开发情况、测试结果及使用方法的文字资料和图表，如程序设计说明书、流程图、用户手册等。软件经营秘密指具有软件秘密性质的经营管理方法以及与经营管理方法密切相关的信息和情报，其中包括管理方法、经营方法、产销策略、客户情报（客户名单、客户需求），以及对软件市场的分析、预测报告和未来的发展规划、招投标中的标底及标书内容等。

**参考答案**

（10）C

**试题（11）**

光纤分为单模光纤和多模光纤，这两种光纤的区别是__（11）__。

（11）A. 单模光纤的数据速率比多模光纤低
B. 多模光纤比单模光纤传输距离更远
C. 单模光纤比多模光纤的价格更便宜
D. 多模光纤比单模光纤的纤芯直径粗

**试题（11）分析**

本题考查有关光纤传输介质的基础知识。

光波在光导纤维中以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径，这样的光纤叫多模光纤（Multi Mode Fiber）。光波在光纤中以什么模式传播，这与芯线的直径、芯线和包层的相对折射率，以及工作波长有关。如果芯线的直径小到光波波长大小，则光纤就成为波导，光在其中无反射地沿直线传播，这种光纤叫单模光纤（Single Mode Fiber），如下图所示。




单模光纤采用激光二极管作为光源，波长分为 1310nm 和 1550nm 两种。单模光纤的纤芯直径为 8.3μm，包层外径为 125μm，可表示为 8.3/125μm。单模光纤只能传导一种模式的光，色散很小，适用于远程通信。如果希望支持万兆传输，而且距离较远，应考虑采用单模光缆。

多模光纤采用 LED 作为光源，波长分为 850nm 和 1300nm 两种。多模光纤的纤芯较粗，有 50μm 和 62.5μm 两种，包层外径 125μm，分别表示为 50/125μm 和 62.5/125μm。多模光纤可传输多种模式的光，但模间色散较大，这就限制了传输信号的频率，而且随着距离的增加，限制会更加严重。多模光纤传输的距离比较近，一般只有几公里。但是多模光纤要比单模光纤价格便宜，如果对传输距离或数据速率要求不高，则可选择多模光缆。

**参考答案**

（11）D

**试题（12）**

下面关于交换机的说法中，正确的是__（12）__。

（12）A. 以太网交换机可以连接运行不同网络层协议的网络

B. 从工作原理上讲，以太网交换机是一种多端口网桥

C. 集线器是一种特殊的交换机

D. 通过交换机连接的一组工作站形成一个冲突域

**试题（12）分析**

本题考查网络交换设备的基础知识。

集线器也是一种物理层设备，虽然它还有检测冲突的作用，但这些操作都属于物理层功能的范围。

网桥是一种数据链路层设备，它处理的对象是数据链路层的协议数据单元——帧，其处理功能包括检查帧的格式、进行差错校验、识别目标地址、选择路由并实现帧的转发等。更准确地说，网桥包含了物理层和数据链路层两个功能层次，所以在以太网中，网桥也能起到延长传输距离的作用。

现代以太网中，更多地使用交换机代替网桥，只有在简单的小型网络中才用微机软件实现网桥的功能。以太网交换机也是一种数据链路层设备，除传统网桥的功能之外，交换机把共享介质变成了专用链路，使得网络的有效数据速率大大提高。

虽然交换机与集线器在外部结构上相似，连接的网络拓扑结构相同，但它们是不同的设备。通过集线器连接的一组工作站形成一个冲突域，其中只能有一个设备发送数据，

其他设备只能接收数据或处于等待状态。用交换机连接的一组工作站可以有多个设备同时发送数据，只要目标站不冲突就可以了。用集线器连接的工作站和用交换机连接的工作站都处于同一广播域中，即网上的所有工作站都能收到广播信息。

**参考答案**

（12）B

**试题（13）**

路由器通过光纤连接广域网的是＿（13）＿。

（13）A. SFP 端口　　B. 同步串行口
C. Console 端口　　D. AUX 端口

**试题（13）分析**

本题考查交换设备端口的基础知识。

路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 口。常见的网络端口有以下几种：

- RJ-45 端口：这种端口通过双绞线连接以太网。10Base-T 的 RJ-45 端口标识为“ETH”，而 100Base-TX 的 RJ-45 端口标识为“10/100bTX”。
- 高速同步串口（Synchronous Serial Port）：在路由器与广域网的连接中，应用最多的是高速同步串行口，这种端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。
- ISDN BRI 端口：ISDN BRI 端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 端口采用 RJ-45 标准，与 ISDN NT1 的连接使用 RJ-45-to-RJ-45 直通线。
- 异步串口（ASYNC）：异步串口主要应用于与 Modem 或 Modem 池的连接，以实现远程计算机通过 PSTN 拨号接入。异步端口的速率不是很高，也不要求同步传输。
- Console 端口：Console 端口通过专用电缆连接至计算机串行口，利用终端仿真程序对路由器进行本地配置。路由器的 Console 端口为 RJ-45 端口。
- AUX 端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Port）。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行转换。AUX 端口支持硬件流控。
- 光纤端口：SC 端口（Subscriber Connector）是一种光纤端口，可提供千兆数据传输速率，通常用于连接服务器的光纤网卡。光纤端口一般是两个，一发一收，光纤跳线也必须是两根。
- GBIC 端口：GBIC 插槽用于安装吉比特端口转换器（Giga Bit-rate Interface Converter，GBIC）。GBIC 模块是将千兆位电信号转换为光信号的热插拔器件，

分为用于级连的 GBIC 模块和用于堆叠的 GBIC 模块。

- SFP 端口：小型机架可插拔设备 SFP（Small Form-factor Pluggable）是 GBIC 的升级版本，其功能基本和 GBIC 一样，但体积减小一半。

**参考答案**

（13）A

**试题（14）**

下面关于 Manchester 编码的叙述中，错误的是__（14）__。

（14）A．Manchester 编码是一种双相码

B．Manchester 编码提供了比特同步信息

C．Manchester 编码的效率为 50%

D．Manchester 编码应用在高速以太网中

**试题（14）分析**

本题考查数据编码的基础知识。

Manchester 编码是一种双相码，即码元取正负两个不同的电平，或者说由正负两个不同的码元表示一个比特，这样编码的效率为 50%，但是由于每个比特中间都有电平跳变，因而提供了丰富的同步信息。这种编码用在数据速率不太高的以太网中。

差分 Manchester 编码也是一种双相码，但是区分“0”和“1”的方法不同。Manchester 编码正变负表示“0”，负变正表示“1”，而差分 Manchester 编码是“0”比特前沿有跳变，“1”比特前沿没有跳变。这种编码用在令牌环网中。

在 Manchester 和差分 Manchester 编码中，每比特中间都有一次电平跳变，因此波特率是数据速率的两倍。对于 100Mb/s 的高速网络，如果采用这类编码方法，就需要 200M 的波特率，其硬件成本是 100M 波特率硬件成本的 5～10 倍。

**参考答案**

（14）D

**试题（15）**

设信道采用 2DPSK 调制，码元速率为 300 波特，则最大数据速率为__（15）__b/s。

（15）A. 300　　B. 600　　C. 900　　D. 1200

**试题（15）分析**

本题考查数字调制的基础知识。

2DPSK 是一种差分相位调制技术，利用前后码元之间的相位变化来表示二进制数据，例如传送“1”时载波相位相对于前一码元的相移为 π，传送“0”时载波相位相对于前一码元的相移为 0。在这种调制方案中，每一码元代表一个比特，由于码元速率为 300 波特，所以最大数据速率为 300b/s。

**参考答案**

（15）A

**试题（16）**

假设模拟信号的最高频率为 6MHz，采样频率必须大于__（16）__时，才能使得到的样本信号不失真。

（16）A. 6MHz　　B. 12MHz　　C. 18MHz　　D. 20MHz

**试题（16）分析**

本题考查脉冲编码调制的基础知识。

用数字脉冲表示模拟数据的编码方法叫作脉冲编码调制（PCM）。这里要经过采样、量化和编码 3 个处理步骤：

- 采样定理：$f \geqslant 2f_{max}$（即采样频率要大于 2 倍的模拟信号频率）。
- 量化等级：根据编码的长度 $n$ 确定量化等级 $N$，$n = \log_2 N$。
- 数字编码：把量化后的样本值变成对应的二进制代码。

由于模拟信号的频率为 6MHz，而采样频率必须大于模拟信号频率的 2 倍，所以应为 12MHz。

**参考答案**

（16）B

**试题（17）**

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，每秒钟传送 100 个字符，则有效数据速率为__（17）__。

（17）A. 500b/s　　B. 700b/s　　C. 770b/s　　D. 1100b/s

**试题（17）分析**

本题考查异步通信的基础知识。

所谓异步通信就是把一个字符作为同步的单位，字符之间插入同步信息。通常一个字符为 7b，加上起始位、奇偶位和 2b 终止位，共 11b，可计算如下：

$$R = \frac{7}{11} \times 11 \times 100 = 700\text{（b/s）}$$

**参考答案**

（17）B

**试题（18）、（19）**

通过 ADSL 访问 Internet，在用户端通过__（18）__和 ADSL Modem 连接 PC，在 ISP 端通过__（19）__设备连接因特网。

（18）A. 分离器　　B. 电话交换机　　C. DSLAM　　D. IP 路由器

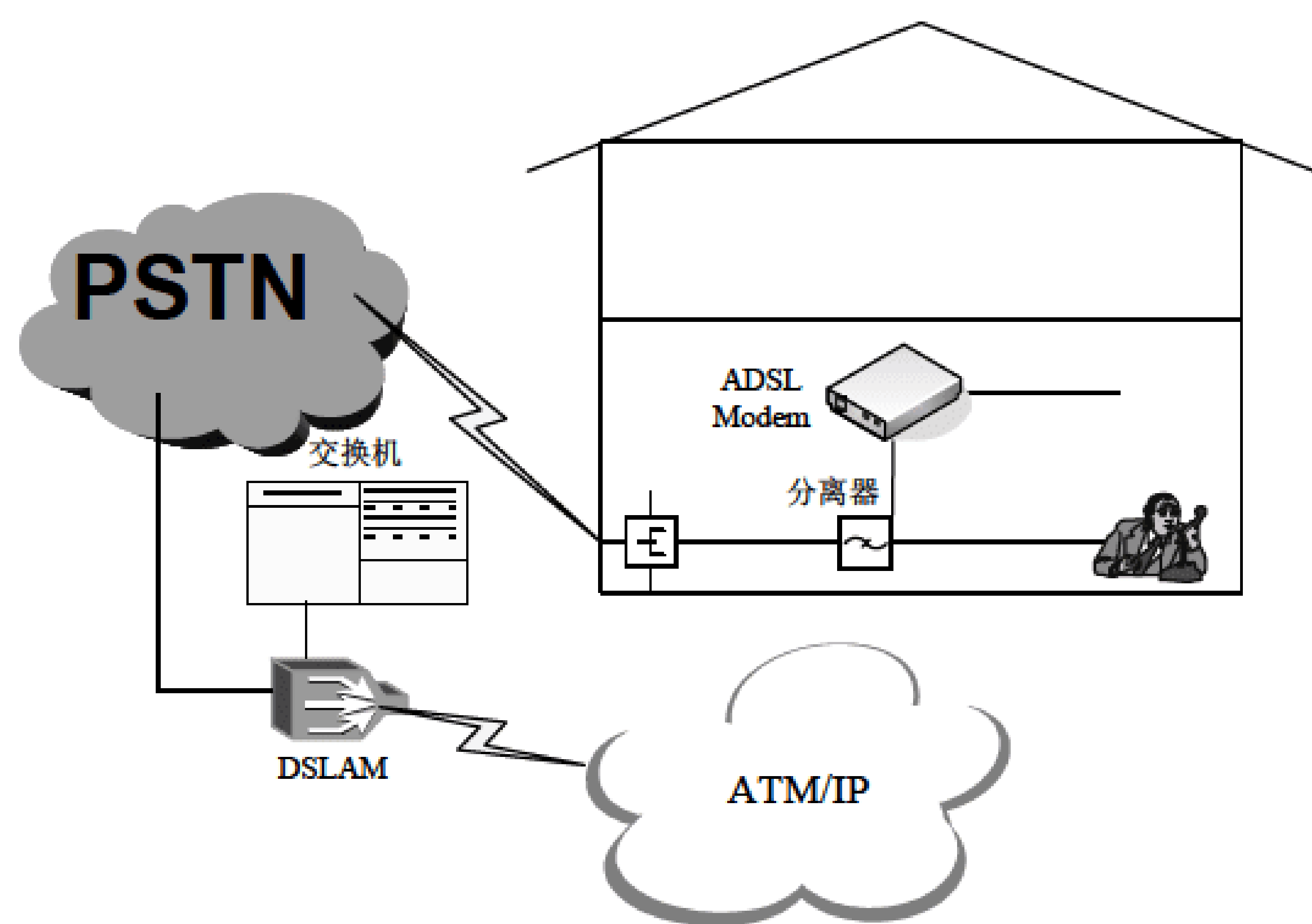
（19）A. 分离器　　B. 电话交换机　　C. DSLAM　　D. IP 路由器

**试题（18）、（19）分析**

本题考查 ADSL 接入知识。

ADSL 接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装 PPPoE

（PPP over Ethernet）或PPPoA（PPP over ATM）客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址，开机即可接入 Internet。




上图表示家庭个人应用的连接线路，PC 通过 ADSL Modem→分离器→入户接线盒→电话线→DSL 接入复用器（DSL Access Multiplexer，DSLAM）连接 ATM 或 IP 网络，而话音线路通过分离器→入户接线盒→电话线→DSL 接入复用器接入电话交换机。

**参考答案**

（18）A　（19）C

**试题（20）**

IPv4 协议头中标识符字段的作用是＿（20）＿。

（20）A. 指明封装的上层协议　　B. 表示松散源路由
　　　C. 用于分段和重装配　　D. 表示提供的服务类型

**试题（20）分析**

本题考查 IP 协议的基础知识。

IP 协议的标识符由主机指定，当源主机对数据分段时，对同一上层协议数据单元划分出的各个数据报指定同样的标识符，目标主机使用这个字段进行重装配。

**参考答案**

（20）C

**试题（21）**

当 TCP 实体要建立连接时，其段头中的＿（21）＿标志置 1。

（21）A. SYN　　B. FIN　　C. RST　　D. URG

**试题（21）分析**

本题考查 TCP 协议的基础知识。

TCP 用三次握手过程建立连接，首先是发起方发送一个 SYN 标志置位的段，其中的发送顺序号为某个值 *X*，称为初始顺序号（Initial Sequence Number，ISN），接收方以

SYN 和 ACK 标志置位的段响应，其中的应答顺序号应为 $X+1$（表示期望从第 $X+1$ 个字节处开始接收数据），发送顺序号为某个值 $Y$（接收端指定的 ISN）。这个段到达发起端后，发起端以 ACK 标志置位，应答顺序号为 $Y+1$ 的段回答，连接就正式建立了，连接建立的同时发起方还可以发送数据，参见下图。

**参考答案**

（21）A

**试题（22）**

UDP 协议在 IP 层之上提供了＿（22）＿能力。

（22）A. 连接管理　　B. 差错校验和重传
C. 流量控制　　D. 端口寻址

**试题（22）分析**

本题考查 UDP 协议的基础知识。

用户数据报协议 UDP 提供无连接的传输服务，由于协议开销少而在很多场合相当实用，特别是网络管理方面，大都使用 UDP 协议。UDP 运行在 IP 协议层之上，由于它不提供连接，所以只是在 IP 协议之上加上端口寻址能力。

**参考答案**

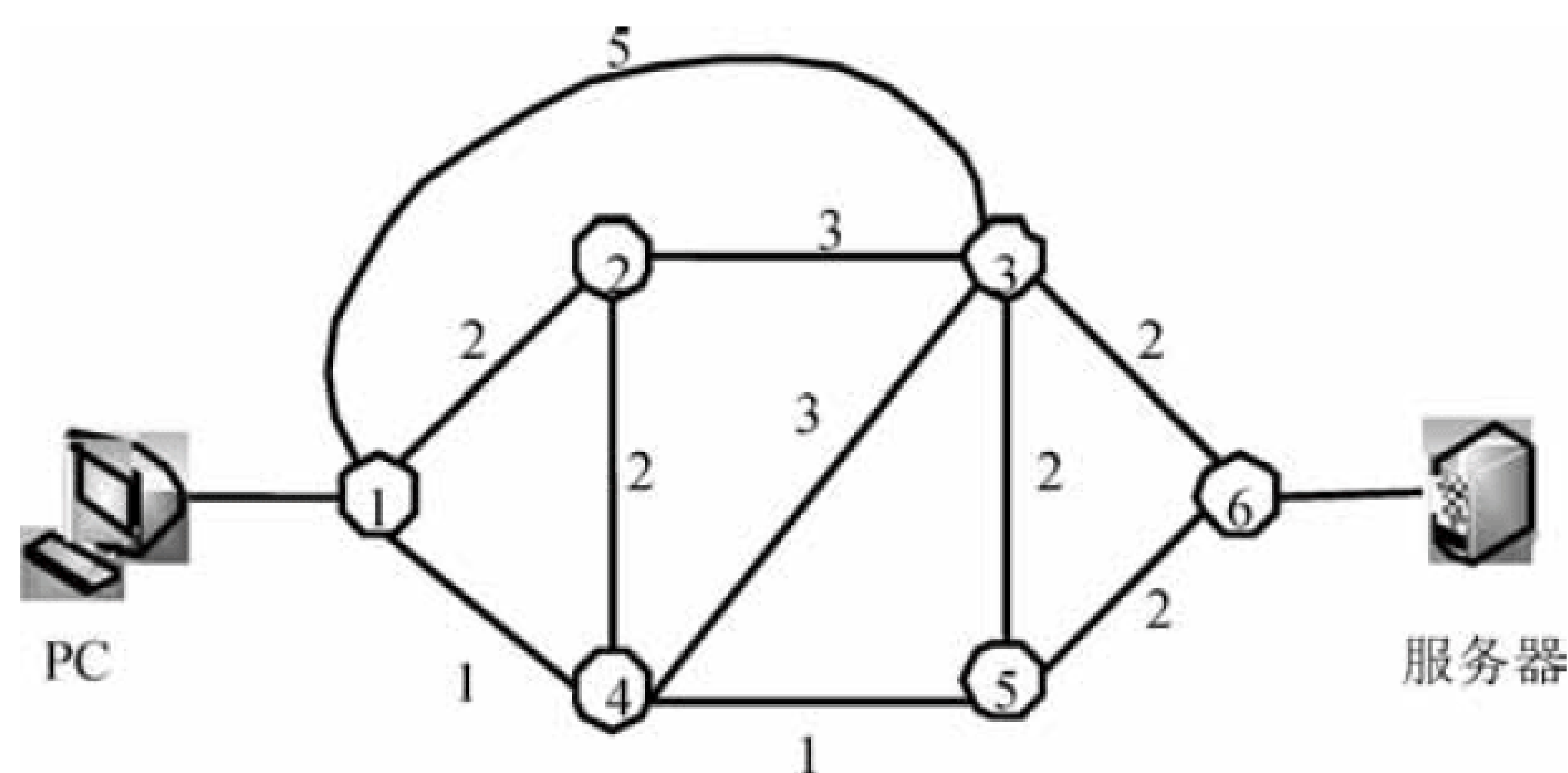
（22）D

**试题（23）、（24）**

网络由 6 个路由器互连而成，路由器之间的链路费用如下图所示，从 PC 到服务器的最短路径是＿（23）＿，通路费用是＿（24）＿。

（23）A. 1→3→6　　B. 1→4→5→6　　C.1→4→3→6　　D. 1→2→4→5→6

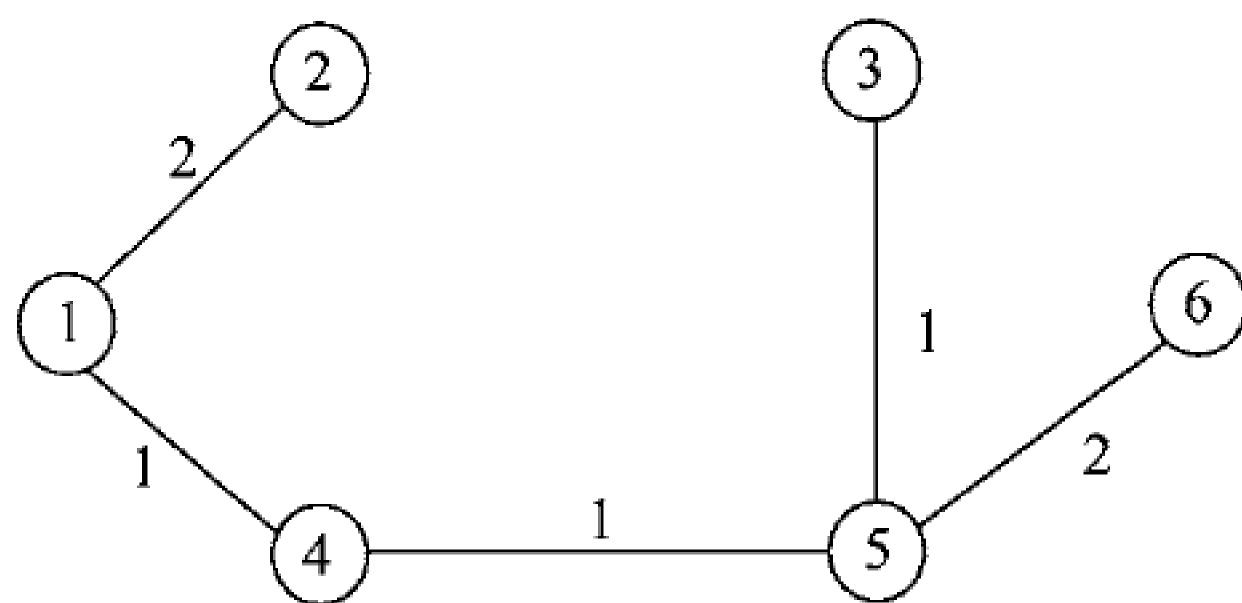
（24）A. 4　　B. 5　　C. 2　　D. 6




**试题（23）、（24）分析**

本题考查最短通路算法的基础知识。

最短通路更一般的说法是最小费用通路，最小费用通路问题可归结为加权图中的最短通路。通常在实际网络中使用的最短通路算法有 Dijkstra 算法和 Bellman-Ford 算法。对本题中的网络采用 Dijkstra 算法，计算得到下图所示的最小生成树，可见从 PC 到服务器的最短路径是 1→4→5→6，通路费用是 4。




**参考答案**

（23）B　（24）A

**试题（25）**

RIPv1 不支持 CIDR，对于运行 RIPv1 协议的路由器，不能设置的网络地址是<u>（25）</u>。

（25）A. 10.16.0.0/8　　B. 172.16.0.0/16

C. 172.22.0.0/18　　D. 192.168.1.0/24

**试题（25）分析**

本题考查路由协议的基础知识。

路由信息协议 RIP 的原型最早出现在 UNIX Berkley 4.3 BSD 中，用于在早期的 ARPAnet 中计算最佳路由。RIP 路由器把自己的路由表广播出去，每个路由器根据邻居发来的路由信息，使用 Bellman-Ford 的距离矢量路由算法更新自己的路由表。RIP 适用于小型网络，因为它允许的跳步数不超过 15 步。

RIPv1 是有类别的协议（classful protocol），这意味着配置 RIPv1 时必须给定 A、B 或 C 类 IP 地址和子网掩码，例如不能把子网掩码 255.255.192.0 用于 B 类网络 172.22.0.0。

**参考答案**

（25）C

**试题（26）**

RIPv2 相对 RIPv1 主要有三方面的改进，其中不包括__（26）__。

（26）A. 使用组播来传播路由更新报文

B. 采用了分层的网络结构

C. 采用了触发更新机制来加速路由收敛

D. 支持可变长子网掩码和路由汇聚

**试题（26）分析**

本题考查路由协议的基础知识。

RIPv2（RFC 1721，1722，1994）是增强了的 RIP 协议，基本上还是一个距离矢量路由协议，但是有三方面的改进：首先，它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次，RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计具有更大的伸缩性。第三，RIPv2 支持认证，使用经过散列的口令字来限制更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

**参考答案**

（26）B

**试题（27）**

IGRP 和 EIGRP 是 Cisco 公司开发的路由协议，它们采用的路由度量方法是__（27）__。

（27）A. 以跳步计数表示通路费用

B. 链路费用与带宽成反比

C. 根据链路负载动态计算通路费用

D. 根据带宽、延迟等多种因素来计算通路费用

**试题（27）分析**

本题考查路由协议的基础知识。

IGRP 是 Cisco 公司开发的路由协议。IGRP 不使用跳步数作为路由度量，虽然在一般情况下可以简化为跳步数。IGRP 的路由度量因素包括带宽、延迟、可靠性、负载和 MTU，其中前两者是默认的，但是可以通过配置加入其他参数。可靠性和负载划分为 1～255 级，可靠性 1 是最低的，可靠性 255 是最高的，负载 1 使用最少，负载 255 是百分之百利用的。MTU 指最大帧长度，在实际运行中，它是一个常数值，通常采用一条通路中最小的 MTU 值。这些因素综合起来作为路由费用的度量，使得 IGRP 可以选择更好的路由。相对于 RIP 的跳步计数，IGRP 协议的路由选择更加合理。

与 IGRP 一样，EIGRP 采用的路由度量（metric）包括带宽、延迟、可靠性、负载等因素，计算方法如下：

metric=[K1×带宽+（K2×带宽）/（256－负载）+K3×延迟]+[K5/（可靠性+K4）]

默认的 K 值如下：

K1=1　　K2=0　　K3=1　　K4=0　　K5=0

当 K5 为 0 时，最后的乘数因子被忽略。这样就得到简化的计算公式：

metric=带宽+延迟

计算结果是一个32 位的数，是通路中各个链路段延迟之和加上带宽，其中带宽经过了规格化：10 的 7 次方除以源和目标之间最小的带宽乘以 256。如果一条路由中各个链路段的传输介质相同，则度量值简化为跳步数。

**参考答案**

（27）D

**试题（28）**

在进行域名解析的过程中，由＿（28）＿获取的解析结果耗时最短。

（28）A. 主域名服务器　　B. 辅域名服务器

C. 缓存域名服务器　　D. 转发域名服务器

**试题（28）分析**

本题考查 DNS 服务器的解析机制。

通常由主域名服务器、辅域名服务器、缓存域名服务器、转发域名服务器进行域名解析。主域名服务器负责维护这个区域的所有域名信息，需要从域管理员构造的本地磁盘文件中加载域信息进行解析。辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务。辅助域名服务器从主域名服务器获得授权，有一个所有域信息的完整拷贝，解析时需要访问本地存储文件。缓存域名服务器可运行域名服务器软件，但是没有域名数据库，它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。转发域名服务器负责所有非本地域名的本地查询，转发域名服务器接到查询请求时，在其缓存中查找，如找不到就把请求依次转发到指定的域名服务器，直到查询到结果为止，否则返回无法映射的结果。

从上述服务器的查询机制中可以看出，缓存域名服务器通过高速缓存的存取进行域名解析，因此获取的解析结果耗时最短。

**参考答案**

（28）C

**试题（29）**

ftp 命令中用来设置客户端当前工作目录的命令是＿（29）＿。

（29）A. get　　B. list　　C. lcd　　D. !list

**试题（29）分析**

本题考查考生对 ftp 命令的掌握程度。

get 或 recv 的功能是下载远程主机的一个文件到自己的计算机上。

list 显示远程计算机上的目录文件和子目录列表。

lcd 命令的功能是更改本地计算机上的工作目录。默认情况下，工作目录是启动 ftp 的目录。

! list 命令的功能是从 ftp 命令行提示符临时退出到 Windows 命令行提示符下，然后运行 list 命令。

**参考答案**

（29）C

**试题（30）**

HTTP 协议中，用于读取一个网页的操作方法为__（30）__。

（30）A. READ　　B. GET　　C. HEAD　　D. POST

**试题（30）分析**

本题考查对 HTTP 命令的掌握程度。

GET 是 HTTP 协议提供的少数操作方法中的一种，其含义是读一个网页。

HEAD 命令用于读取网页头信息。

POST 命令用于把消息加到指定的网页上。不存在 READ 命令。

**参考答案**

（30）B

**试题（31）**

在 Linux 系统中可用 ls -al 命令列出文件列表，__（31）__列出的是一个符号连接文件。

（31）A. drwxr-xr-x　2　root　root　220　2009-04-14 17:30　doc

B. -rw-r--r--　1　root　root　1050　2009-04-14 17:30　doc1

C. lrwxrwxrwx　1　root　root　4096　2009-04-14 17:30　profile

D. drwxrwxrwx　4　root　root　4096　2009-04-14 17:30　protocols

**试题（31）分析**

本题考查 Linux 系统下文件属性的基本概念。其中符号连接文件的属性用 l 表示。

**参考答案**

（31）C

**试题（32）**

Linux 系统中，下列关于文件管理命令 cp 与 mv 说法正确的是__（32）__。

（32）A. 没有区别

B. mv 操作不增加文件个数

C. cp 操作不增加文件个数

D. mv 操作不删除原有文件

**试题（32）分析**

本题考查 Linux 系统下文件操作命令 cp 和 mv 的基本概念。

其中 mv 命令是移动文件，不增加文件个数。

**参考答案**

（32）B

**试题（33）**

Linux 系统中，默认安装 DHCP 服务的配置文件为__（33）__。

（33）A. /etc/dhcpd.conf　　B. /etc/dhcp.conf

C. /etc/dhcpd.config　　D. /etc/dhcp.config

**试题（33）分析**

本题考查 Linux 系统下 DHCP 服务的配置文件存放位置。

**参考答案**

（33）A

**试题（34）**

默认情况下，远程桌面用户组（Remote Desktop Users）成员对终端服务器__（34）__。

（34）A. 具有完全控制权

B. 具有用户访问权和来宾访问权

C. 仅具有来宾访问权

D. 仅具有用户访问权

**试题（34）分析**

本题考查 Windows 操作系统中远程桌面组用户的默认权限。

默认情况下，远程桌面用户组成员具有用户访问权和来宾访问权。

**参考答案**

（34）B

**试题（35）**

Windows Server 2003 采用了活动目录（Active Directory）对网络资源进行管理，活动目录需安装在__（35）__分区。

（35）A. FAT16　　B. FAT32　　C. ext2　　D. NTFS

**试题（35）分析**

本题考查 Windows 操作系统活动目录的基本概念。活动目录必须安装在 NTFS 分区。

**参考答案**

（35）D

**试题（36）**

Linux 系统中，__（36）__服务的作用与 Windows 的共享文件服务作用相似，提供基于网

络的共享文件/打印服务。

（36）A. Samba　　B. Ftp　　C. SMTP　　D. Telnet

**试题（36）分析**

本题考查 Linux 系统中 SAMBA 服务的基本概念。

**参考答案**

（36）A

**试题（37）**

以下关于 DHCP 协议的描述中，错误的是__（37）__。

（37）A. DHCP 客户机可以从外网段获取 IP 地址

B. DHCP 客户机只能收到一个 dhcpoffer

C. DHCP 不会同时租借相同的 IP 地址给两台主机

D. DHCP 分配的 IP 地址默认租约期为 8 天

**试题（37）分析**

本题考查考生对 DHCP 协议的掌握程度。

借助中继代理，DHCP 客户机可以从外网段获取 IP 地址；DHCP 不会同时租借相同的 IP 地址给两台主机；默认情况下 DHCP 分配的 IP 地址租约期为 8 天；DHCP 客户机可以收到多个 dhcpoffer，通常从中选择最先到达的作为本机的 IP 地址。

**参考答案**

（37）B

**试题（38）**

在某台 PC 上运行 ipconfig /all 命令后得到如下结果，下列说法中错误的是__（38）__。

```
C:\Documents and Settings\wy>ipconfig /all

Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ethernet NIC
        Physical Address. . . . . . . . . : 00-1F-D0-83-AA-0F
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 215.155.3.153
        Subnet Mask . . . . . . . . . . . : 255.255.255.192
        Default Gateway . . . . . . . . . : 215.155.3.190
        DHCP Server . . . . . . . . . . . : 152.50.255.1
        DNS Servers . . . . . . . . . . . : 8.8.8.8
                                            252.117.112.3
        Lease Obtained. . . . . . . . . . : 2010-8-9 1:19:55
        Lease Expires . . . . . . . . . . : 2010-8-9 9:19:55
```

（38）A. 该 PC 的 IP 地址的租约期为 8 小时

B. 该 PC 访问 Web 网站时最先查询的 DNS 服务器为 8.8.8.8

C. 接口 215.155.3.190 和 152.50.255.1 之间使用了 DHCP 中继代理

D. DHCP 服务器 152.50.255.1 可供分配的 IP 地址数只能为 61

**试题（38）分析**

本题考查考生对本机配置信息的掌握程度。

IP 地址的发放时间为 2010-8-9 1:19:55，释放时间为 2010-8-9 9:19:55，由此可知该 PC 的 IP 地址的租约期为 8 小时，选项 A 说法正确。

首选 DNS 服务器地址为 8.8.8.8，由此可知该 PC 访问 Web 网站时最先查询的 DNS 服务器为 8.8.8.8，故选项 B 说法正确。

DHCP 服务器地址为 152.50.255.1，本机地址为 215.155.3.155，和 DHCP 服务器不属同一网段，因此接口 215.155.3.190 和 152.50.255.1 之间使用了 DHCP 中继代理，选项 C 说法正确。

DHCP 服务器 215.155.3.153/26 可供分配的 IP 地址数为 61，但其地址池可以分配多个网段，选项 D 说法不正确。

**参考答案**

（38）D

**试题（39）**

在 Windows 系统中需要重新从 DHCP 服务器获取 IP 地址时，可以使用＿（39）＿命令。

（39）A. ifconfig -a　　B. ipconfig

C. ipconfig/all　　D. ipconfig/renew

**试题（39）分析**

本题考查考生对 ipconfig 命令的运用。

ipconfig 是最常用的 Windows 实用程序，可以显示所有网卡的 TCP/IP 配置参数，刷新动态主机配置协议（DHCP）和域名系统（DNS）的设置。

ipconfig/all 用于显示所有网卡的 TCP/IP 配置信息。如果没有该参数，则只显示各个网卡的 IP 地址、子网掩码和默认网关地址。

ipconfig/renew 用于更新网卡的 DHCP 配置，如果使用标识符 Adapter 说明了网卡的名字，则只更新指定网卡的配置，否则就更新所有网卡的配置。

**参考答案**

（39）D

**试题（40）**

IIS 6.0 将多个协议结合起来组成一个组件，其中不包括＿（40）＿。

（40）A. POP3　　B. SMTP　　C. FTP　　D. DNS

**试题（40）分析**

本题考查考生对 IIS 6.0 组件的了解程度。

可以利用因特网信息服务器（Internet Information Server，IIS）来构建 WWW 服务器、FTP 服务器、SMTP 服务器和 POP3 服务器等。IIS 服务将 HTTP 协议、FTP 协议与 Windows Server 2000 出色的管理功能和安全特性结合起来，提供了一个功能全面的软件包，面向不同的应用领域给出了 Internet/Intranet 服务器解决方案。

**参考答案**

（40）D

**试题（41）**

按照 RSA 算法，若选两奇数 $p$=5，$q$=3，公钥 $e$=7，则私钥 $d$ 为__（41）__。

（41）A. 6　　B. 7　　C. 8　　D. 9

**试题（41）分析**

本题考查 RSA 的算法知识。

RSA 是一种公钥加密算法，它按照下面的要求选择公钥和密钥：

1）选择两个大素数 $p$ 和 $q$（大于 $10^{100}$）

2）令 $n=p*q$ 和 $z=(p-1)*(q-1)$

3）选择 $d$ 与 $z$ 互质

4）选择 $e$，使 $e*d=1(\bmod z)$

从题中举例数据 $p$=5、$q$=3、$e$=7 可得：

$n=5*3=15$；

$z=(5-1)*(3-1)=8$；

$7*d=1(\bmod 8)$；

将题中 4 个选项代入上式可知，只有 $d$=7 满足要求。

**参考答案**

（41）B

**试题（42）、（43）**

在 SNMP 中，管理进程查询代理中一个或多个变量的值所用报文名称为__（42）__，该报文的缺省目标端口是__（43）__。

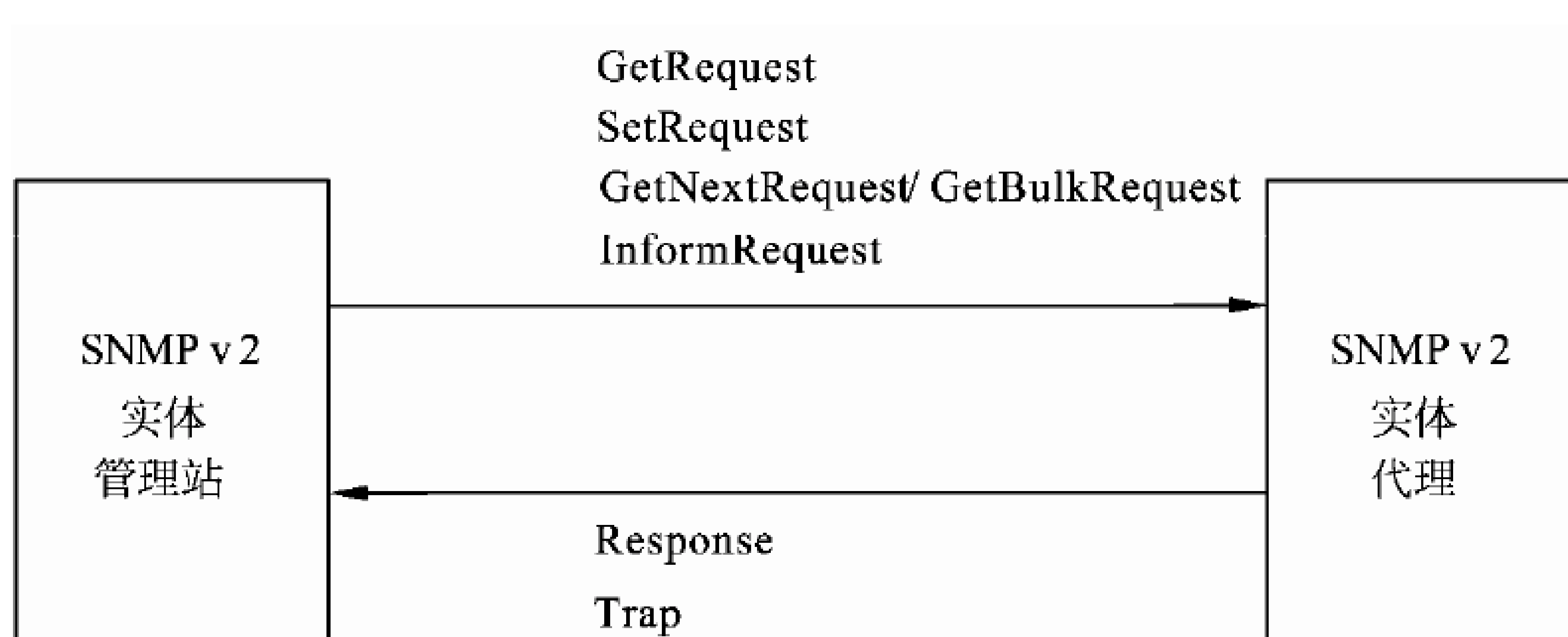
（42）A. get-request　　B. set-request　　C. get-response　　D. trap

（43）A. 160　　B. 161　　C. 162　　D. 163

**试题（42）、（43）分析**

本题考查网络管理协议 SNMP 的基础知识。

在 SNMP 管理中，管理站和代理之间交换的管理信息构成了 SNMP 报文。SNMP 报文包括 GetRequest、GetNextRequest、GetBulkRequest（SNMPv2）、SetRequest、InformRequest（SNMPv2）和 Trap、Response，如下图所示。




其中选项（A）get-request 可用于管理进程查询代理中一个或多个变量的值。

根据 SNMP 协议规定（RFC1157），管理站发送报文的协议为 UDP，目的端口为 161，代理发送的 Trap 报文的目的端口为 162。所以 get-request 报文的缺省目的端口是 161。

**参考答案**

（42）A　（43）B

**试题（44）**

Windows 系统中，路由跟踪命令是__（44）__。

（44）A．tracert　　B．traceroute　　C．routetrace　　D．trace

**试题（44）分析**

本题考查 Windows 系统中的网络操作命令。

查询 Windows 帮助可得以下信息：

```
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list.
    -w timeout          Wait timeout milliseconds for each reply.
```

**参考答案**

（44）A

**试题（45）、（46）**

报文摘要算法 MD5 的输出是__（45）__位，SHA-1 的输出是__（46）__位。

（45）A. 56　　B. 128　　C. 160　　D. 168

（46）A. 56　　B. 128　　C. 160　　D. 168

**试题（45）、（46）分析**

本题考查网络安全中报文摘要算法的相关知识。

MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分

组级联后将生成一个128位散列值。

SHA（安全散列算法）是美国国家安全局设计、美国国家标准与技术研究院（NIST）发布的一系列密码散列函数。其中SHA-1 会从一个最大 $2^{64}$ 位元的信息中产生一串 160 位元的摘要。

**参考答案**

（45）B （46）C

**试题（47）**

下列隧道协议中工作在网络层的是__（47）__。

（47）A．SSL　　B．L2TP　　C．IPSec　　D．PPTP

**试题（47）分析**

本题考查隧道协议的综合知识。

隧道技术是VPN的基本技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。

第二层隧道协议是先把各种网络协议封装到PPP中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec（IP Security）等。IPSec由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法、确定服务所使用密钥等服务，从而在IP层（网络层）提供安全保障。

**参考答案**

（47）C

**试题（48）**

IEEE 802.11i所采用的加密算法为__（48）__。

（48）A．DES　　B．3DES　　C．IDEA　　D．AES

**试题（48）分析**

本题考查加密算法的应用。

IEEE 802.11i是IEEE为了弥补802.11脆弱的安全加密功能（WEP）而制定的修正案，于2004年7月完成。其中定义了基于AES的全新加密协议CCMP（CTR with CBC-MAC Protocol）。

**参考答案**

（48）D

**试题（49）、（50）**

公钥体系中，私钥用于__（49）__，公钥用于__（50）__。

（49）A．解密和签名　　B．加密和签名

C．解密和认证　　D．加密和认证

（50）A．解密和签名　　B．加密和签名

C．解密和认证　　D．加密和认证

**试题（49）、（50）分析**

本题考查公钥体系的理解和应用。

1976 年斯坦福大学的 Diffie 和 Hellman 提出了使用不同的密钥进行加密和解密的公钥加密算法。设 P 为明文，C 为密文，E 为公钥控制的加密算法，D 为私钥控制的解密算法，这些参数满足下列 3 个条件：

（1）D（E（P））=P

（2）不能由 E 导出 D

（3）选择明文攻击（选择任意明文-密文对以确定未知的密钥）不能破解 E

加密时计算 C=E（P），解密时计算 P=D（C）。加密和解密是互逆的。用公钥加密、私钥解密，可实现保密通信；用私钥加密、公钥解密，可实现数字签名。

**参考答案**

（49）A　（50） D

**试题（51）**

网络 172.21.136.0/24 和 172.21.143.0/24 汇聚后的地址是＿（51）＿。

（51）A. 172.21.136.0/21　　B. 172.21.136.0/20

C. 172.21.136.0/22　　D. 172.21.128.0/21

**试题（51）分析**

本题考查 IP 地址计算的基础知识。

网络 172.21.136.0/24 的二进制表示为：　**10101100 00010101 10001000** 00000000

网络 192.21.143.0/24 的二进制表示为：　**10101100 00010101 10001111** 00000000

所以汇聚后的地址为：**10101100 00010101 10001**000 00000000，即 172.21.136.0/21。

**参考答案**

（51）A

**试题（52）**

如果子网 172.6.32.0/20 再划分为 172.6.32.0/26，则下面的结论中正确的是＿（52）＿。

（52）A. 划分为 1024 个子网　　B. 每个子网有 64 台主机

C. 每个子网有 62 台主机　　D. 划分为 2044 个子网

**试题（52）分析**

本题考查 IP 地址计算的基础知识。网络 172.6.32.0/20 划分为 172.6.32.0/26，即

网络 172.6.132.0/20 的二进制表示为：　**10101100 00000110 10000100** 00000000

网络 172.6.132.0/26 的二进制表示为：　**10101100 00000110 10000100 00000000**

**10101100 00000110 10000100 01000000**

**10101100 00000110 10000100 10000000**

**10101100 00000110 10000100 11000000**

……………………………………………..

**10101100 00000110 10000111 11000000**

共分成了16个子网，每个子网的主机地址部分有6位。除去全0和全1，有62个主机地址。

**参考答案**

（52）C

**试题（53）**

下面给出的网络地址中，属于私网地址的是__（53）__。

（53）A. 119.12.73.214　　B. 192.32.146.23

C. 172.34.221.18　　D. 10.215.34.124

**试题（53）分析**

本题考查IP地址的基础知识。

私网地址不能在公网上出现，只能用在内部网络中，所有的路由器都不转发目标地址为私网地址的数据报。下面的地址都是私网地址：

10.0.0.0～10.255.255.255　　1个A类地址

172.16.0.0～172.31.255.255　　16个B类地址

192.168.0.0～192.168.255.255　　256个C类地址

**参考答案**

（53）D

**试题（54）**

IP地址172.17.16.255/23是一个__（54）__。

（54）A. 网络地址　　B. 主机地址

C. 定向广播地址　　D. 不定向广播地址

**试题（54）分析**

本题考查IP地址的基础知识。

IP地址172.17.16.255/23的二进制表示为：**10101100 00010001 00010000** 11111111所以应该是主机地址。

**参考答案**

（54）B

**试题（55）**

给定一个C类网络192.168.1.0/24，要在其中划分出3个60台主机的网段和2个30台主机的网段，则采用的子网掩码应该分别为__（55）__。

（55）A. 255.255.255.128 和 255.255.255.224　　B. 255.255.255.128 和 255.255.255.240
　　C. 255.255.255.192 和 255.255.255.224　　D. 255.255.255.192 和 255.255.255.240

**试题（55）分析**

本题考查 IP 地址计算的基础知识。

要在网络 192.168.1.0/24 中划分出 3 个 60 台主机的网段和 2 个 30 台主机的网段，首先可采用子网掩码 255.255.255.192，得到 3 个子网：

**11000000 10101000 00000001 00000000**
**11000000 10101000 00000001 01000000**
**11000000 10101000 00000001 10000000**

然后采用子网掩码和 255.255.255.224，得到两个子网：

**11000000 10101000 00000001 11000000**
**11000000 10101000 00000001 11100000**

**参考答案**

（55）C

**试题（56）**

在交换机上同时配置了使能口令（enable password）和使能密码（enable secret），起作用的是__（56）__。

（56）A. 使能口令　　B. 使能密码　　C. 两者都不能　　D. 两者都可以

**试题（56）分析**

本题考查交换机的配置命令。

在交换机中可以配置使能口令和使能密码，两者的区别是使能口令以明文显示，而使能密码以密文显示。一般只需配置一个就可以了，当两者同时配置时，后者生效，参见下面的例子。

```
Switch>                                    (用户执行模式提示符)
Switch >enable                             (进入特权模式)
Switch #                                   (特权模式提示符)
Switch #config terminal                    (进入配置模式)
Switch(config)#                            (配置模式提示符)
Switch(config)#enable password cisco       (设置 enable password 为 cisco)
Switch(config)#enable secret cisco1        (设置 enable secret 为 cisco1)
Switch(config)#hostname C2950              (设置主机名为 C2950)
C2950(config)#end                          (退回到特权模式)
C2950#
```

**参考答案**

（56）B

**试题（57）**

以下的命令中，可以为交换机配置默认网关地址的是__（57）__。

（57）A. 2950(config)# default-gateway 192.168.1.254

B. 2950(config-if)# default-gateway 192.168.1.254

C. 2950(config)#ip default-gateway 192.168.1.254

D. 2950(config-if)#ip default-gateway 192.168.1.254

**试题（57）分析**

本题考查交换机的配置命令。

在全局配置模式下可以设置交换机的 IP 地址、默认网关、域名等信息，这些信息是用来管理交换机的，与连接在交换机上的计算机或其他设备无关，参见下面的例子。

```
C2950(config)#ip address 192.168.1.1 255.255.255.0   (设置交换机 IP 地址)
C2950(config)#ip default-gateway 192.168.1.254       (设置默认网关)
C2950(config)#ip domain-name cisco.com               (设置域名)
C2950(config)#ip name-server 200.0.0.1               (设置域名服务器)
C2950(config)#end
```

**参考答案**

（57）C

**试题（58）**

在路由器配置过程中，要查看用户输入的最后几条命令，应该键入__（58）__。

（58）A. show version　　B. show commands

C. show previous　　D. show history

**试题（58）分析**

本题考查路由器的显示命令。

查看键入命令的历史可以用命令 Router #show history，也可以使用上下箭头键，或者^p 和^n。其他显示命令如下表所示。

| 任　务 | 命　令 |
|---|---|
| 查看版本及引导信息 | show version |
| 查看运行设置 | show running-config |
| 查看开机设置 | show startup-config |
| 显示端口信息 | show interface *type slot/number* |
| 显示路由信息 | show ip route |

**参考答案**

（58）D

**试题（59）**

在交换机之间的链路中，能够传送多个 VLAN 数据包的是__（59）__。

（59）A. 中继连接　　B. 接入链路

C. 控制连接　　　　　　　　D. 分支链路

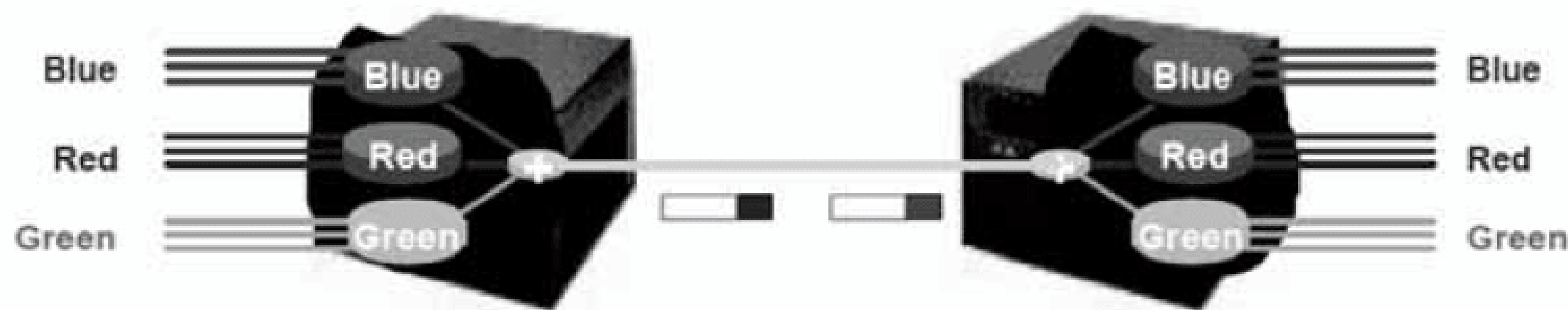
**试题（59）分析**

本题考查 VLAN 的基础知识。

在划分成 VLAN 的交换局域网中，交换机端口之间的连接分为两种：接入链路连接（Access-Link Connection）和中继连接（Trunk Connection）。接入链路只能连接具有标准以太网卡的设备，只能解释以太帧，也只能传送属于单个 VLAN 的数据包。任何连接到接入链路的设备都属于同一广播域。

中继连接能够传送多个 VLAN 的数据包。为了支持中继连接，应该修改原来的以太网数据包，在其中加入 VLAN 标记，以区分属于不同 VLAN 的广播域。例如，VLAN1 中的设备发出一个广播包，这个广播包在交换网络中传送，所有的交换机都必须识别 VLAN1 的标识符，以便把该数据包转发到属于 VLAN1 的端口去。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个 VLAN。在进入中继端口时，交换机在数据包中加入 VLAN 标记。这样，在中继链路另一端的交换机不仅根据目标地址进行转发，而且要根据数据包所属的 VLAN 进行转发决策。下图用不同的颜色表示不同 VLAN 的帧，这些帧共享一条中继链路。




为了与接入链路设备兼容，在数据包进入接入链路连接的设备时，交换机要删除 VLAN 标记，恢复原来的帧结构。添加和删除 VLAN 标记的过程是由交换机中的专用硬件自动实现的。从用户角度看，数据源产生标准的以太帧，目标接收的也是标准的以太帧，VLAN 标记对用户是透明的。

通常的 PC 网卡不支持中继连接，但是也有的网卡支持中继连接。如果一个服务器要接受多个 VLAN 的访问，并直接连接在交换机上，则应该在服务器中插入支持中继连接的网卡，这种配置比通过路由器转发效率高。

**参考答案**

（59）A

**试题（60）**

要实现 VTP 动态修剪，在 VTP 域中的所有交换机都必须配置成__（60）__。

（60）A. 服务器　　　　　　　　B. 服务器或客户机

C. 透明模式　　　　　　　　D. 客户机

**试题（60）分析**

本题考查 VTP 协议的基础知识。

VLAN 中继协议（VLAN Trunking Protocol，VTP）是 Cisco 公司的专利协议。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为 3 种：

（1）服务器模式（Server）：交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

（2）客户机模式（Client）：在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

（3）透明模式（Transparent）：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

**参考答案**

（60）A

**试题（61）**

能进入 VLAN 配置状态的交换机命令是<u>（61）</u>。

（61）A. 2950(config)# vtp pruning　　B. 2950# vlan database

C. 2950(config)# vtp server　　D. 2950(config)# vtp mode

**试题（61）分析**

本题考查交换机的配置命令。

根据 IOS 版本的不同，2950 可以用两种方式配置。在老版本中是从特权模式（Privilege EXEC）开始配置的，使用下面的命令：

```
2950# vlan database                                  （从特权模式进入 VLAN 配置模式）
2950(vlan)# vtp domain VTP_domain_name               （指定 VTP 域名）
2950(vlan)# vtp server|client|transparent            （指定交换机的工作模式）
2950(vlan)# vtp password VTP_password                （配置 VTP 口令）
2950(vlan)# vtp pruning                              （启用 VTP 修剪）
2950(vlan)# abort                                    （返回特权模式，不保存配置结果）
```

或者

```
2950(vlan)# exit                                     （返回特权模式，并保存配置结果）
```

如果使用的是 IOS 12.1(11) EA1 以后的新版本，则从全局配置模式开始：

```
2950(config)# vtp domain VTP_domain_name
2950(config)# vtp mode server|client|transparent
2950(config)# vtp password VTP_password
2950(config)# vtp pruning
```

**参考答案**

（61）B

**试题（62）**

以太网协议可以采用非坚持型、坚持型和 P 坚持型 3 种监听算法。下面关于这 3 种算法的描述中，正确的是（62）。

（62）A. 坚持型监听算法的冲突概率低，但可能引入过多的信道延迟

B. 非坚持型监听算法的冲突概率低，但可能浪费信道带宽

C. P 坚持型监听算法实现简单，而且可以达到最好性能

D. 非坚持型监听算法可以及时抢占信道，减少发送延迟

**试题（62）分析**

本题考查以太网协议的基础知识。以太网监听算法有如下 3 种：

① 非坚持型监听算法：若信道忙，则放弃监听，后退一段随机时间后再试图重新发送。这种方法重新冲突的概率低，但可能引入过多的信道延迟，浪费信道的带宽。

② 坚持型监听算法：若信道忙，则继续监听，直到信道空闲就可发送。这种方法发生冲突的概率高，但可以减少发送延迟。

③ P 坚持型监听算法：若信道忙，则以概率 P 继续监听，或以概率 1-P 放弃监听并后退一段随机时间，再试图重新发送。这种方法具有以上两种方法的优点，但是算法复杂，P 值的大小对网络的性能有较大影响。

**参考答案**

（62）B

**试题（63）**

以太网帧格式如下图所示，其中的“长度”字段的作用是（63）。

| 前导字段 | 帧起始符 | 目的地址 | 源地址 | 长度 | 数据 | 填充 | 校验和 |
|---|---|---|---|---|---|---|---|

（63）A. 表示数据字段的长度

B. 表示封装的上层协议的类型

C. 表示整个帧的长度

D. 既可以表示数据字段长度，也可以表示上层协议的类型

**试题（63）分析**

本题考查以太网协议的基础知识。

最早采用 CSMA/CD 协议的网络是 Xerox 公司的以太网。1981 年，DEC、Intel 和

Xerox 三家公司制定了 DIX 以太网标准，使这一技术得到越来越广泛的应用。IEEE 802 委员制定局域网标准时参考了以太网标准，并增加了几种新的传输介质。

早期的 802.3 帧格式与 DIX 以太网不同，DIX 以太网用类型字段指示所封装的上层协议，而 IEEE 802.3 为了通过 LLC 实现向上复用，用长度字段取代了类型字段。实际上，这两种格式可以并存，两个字节可表示的数字值范围是 0～65 535，长度字段的最大值是 1500，因此 1501～65 535 之间的值都可以用来标识协议类型。事实上，这个字段的 1536～65 535（0x0600～0xFFFF）之间的值都被保留作为类型值，而 0～1500 则被用作长度的值。许多高层协议（例如 TCP/IP、IPX、DECnet 4）使用 DIX 以太网帧格式，而 IEEE 802.3/LLC 在 AppleTalk-2 和 NetBIOS 中得到应用。

IEEE 802.3x 工作组为了支持全双工操作，开发了流量控制算法，这使得帧格式出现了一些变化，新的 MAC 协议使用类型字段来区分 MAC 控制帧和其他类型的帧。IEEE 802.3x 在 1997 年 2 月成为正式标准，使得原来的“以太网使用类型字段而 IEEE 802.3 使用长度字段”的差别消失。

**参考答案**

（63）D

**试题（64）**

下面列出的 4 种快速以太网物理层标准中，使用两对 5 类无屏蔽双绞线作为传输介质的是__（64）__。

（64）A. 100Base-FX　　B. 100Base-T4
C. 100Base-TX　　D. 100Base-T2

**试题（64）分析**

本题考查快速以太网的基础知识。

1995 年 100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布，这是基于 10Base-T 和 10Base-F 技术、在基本布线系统不变的情况下开发的高速局域网标准。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为 62.5μm，包层直径为 125μm，单模光线芯线直径为 8μm，包层直径也是 125μm。

| 标　准 | 传 输 介 质 | 特 性 阻 抗 | 最 大 段 长 |
|---|---|---|---|
| 100Base-TX | 2 对 5 类 UTP | 100Ω | 100m |
| | 2 对 STP | 150Ω | |
| 100Base-FX | 一对多模光纤 MMF | 62.5/125μm | 2km |
| | 一对单模光纤 SMF | 8/125μm | 40km |
| 100Base-T4 | 4 对 3 类 UTP | 100Ω | 100m |
| 100Base-T2 | 2 对 3 类 UTP | 100Ω | 100m |

**参考答案**

（64）C

**试题（65）**

用于工业、科学和医疗方面的免许可证的微波频段有多个，其中世界各国通用的ISM频段是__（65）__。

（65）A. 902～928MHz　　B. 868～915MHz
C. 5725～5850MHz　　D. 2400～2483.5MHz

**试题（65）分析**

本题考查无线通信的基础知识。

世界各国都划出一些无线频段，用于工业、科学研究和微波医疗方面。应用这些频段无需许可证，只要低于一定的发射功率（一般为 1w）即可自由使用。美国有 3 个 ISM 频段（902～928MHz、2400～2483.5MHz、5725～5850MHz），2.4GHz 为各国共同的 ISM 频段。频谱越高，潜在的带宽也越大。另外，还要考虑可能出现的干扰。有些设备（例如无绳电话、无线麦克、业余电台等）的工作频率为 900MHz。还有些设备运行在 2.4GHz 上，典型的例子就是微波炉，它使用久了会泄露更多的射线。目前看来，在 5.8GHz 频带上还没有什么竞争。但是频谱越高，设备的价格就越贵。

**参考答案**

（65）D

**试题（66）**

2009 年发布的__（66）__标准可以将 WLAN 的传输速率由 54Mb/s 提高到 300～600Mb/s。

（66）A. IEEE 802.11n　　B. IEEE 802.11a
C. IEEE 802.11b　　D. IEEE 802.11g

**试题（66）分析**

本题考查 WLAN 的基础知识。

自从 1997 年 IEEE 802.11 标准实施以来，先后有二十多个标准出台，其中802.11a、802.11b 和802.11g采用了不同的通信技术，使得数据传输速率不断提升，但是与有线网络相比仍然存在一定差距。随着 2009 年 9 月 11 日 IEEE 802.11n 标准的正式发布，这一差距正在缩小，有望使得一些杀手级的应用能够在 WLAN 平台上畅行无阻。

802.11n 可以将 WLAN 的传输速率由目前 802.11a/802.11g 的 54Mb/s 提高到 300Mb/s，甚至 600Mb/s。这个成就主要得益于 MIMO 与 OFDM 技术的结合。应用先进的无线通信技术，不但提高了传输速率，也极大地提升了传输质量。

**参考答案**

（66）A

**试题（67）**

网络系统生命周期可以划分为5个阶段，实施这5个阶段的合理顺序是＿（67）＿。

（67）A. 需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段

B. 需求规范、逻辑网络设计、通信规范、物理网络设计、实施阶段

C. 通信规范、物理网络设计、需求规范、逻辑网络设计、实施阶段

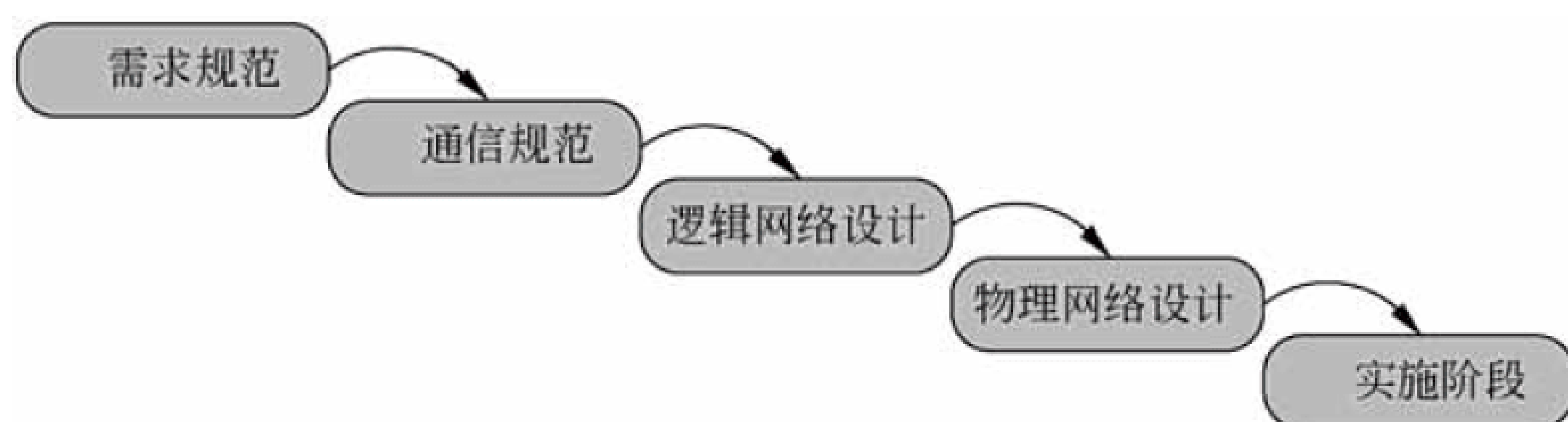
D. 通信规范、需求规范、逻辑网络设计、物理网络设计、实施阶段

**试题（67）分析**

本题考查网络规划和设计方面的基础知识。一个网络系统从构思开始，到最后被淘汰的过程称为网络生命周期。一般来说，网络生命周期至少应包括网络系统的构思和计划、分析和设计、运行和维护的全过程。网络系统的生命周期与软件工程中的软件生命周期类似，首先它是一个循环迭代的过程，每次循环迭代的动力都来自网络应用需求的变更。其次，每次循环过程中，都存在需求分析、规划设计、实施调试和运营维护等多个阶段。一般来说，网络规模越大，则可能经历的循环周期也越长。

每一个迭代周期都是网络重构的过程，不同的网络设计方法，对迭代周期的划分方式是不同的，拥有不同的网络文档模板，但是实施后的效果都满足了用户的网络需求。常见的迭代周期构成可分为如下5个阶段：需求规范阶段、通信规范阶段、逻辑网络设计阶段、物理网络设计阶段及实施阶段。

在这5个阶段中，每个阶段都是一个工作环节，每个环节完毕后才能进入下一个环节，类似于软件工程中的“瀑布模型”，形成了特定的工作流程。如下图所示。




按照这种流程构建网络，在下一个阶段开始之前，前一阶段的工作已经完成，一般情况下，不允许返回到前面的阶段。

**参考答案**

（67）A

**试题（68）**

大型局域网通常划分为核心层、汇聚层和接入层，以下关于各个网络层次的描述中，不正确的是＿（68）＿。

（68）A. 核心层承担访问控制列表检查

B. 汇聚层定义了网络的访问策略

C. 接入层提供局域网络接入功能

D. 接入层可以使用集线器代替交换机

**试题（68）分析**

本题考查局域网体系结构的基础知识。

大型局域网的层次结构是将局域网络划分成不同的功能层次，例如划分成核心层、汇聚层和接入层，通过与核心设备互连的路由器接入广域网。

在三层模型中，核心层提供不同区域之间的高速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

**参考答案**

（68）A

**试题（69）**

网络系统设计过程中，逻辑网络设计阶段的任务是＿（69）＿。

（69）A. 依据逻辑网络设计的要求，确定设备的物理分布和运行环境

B. 分析现有网络和新网络的资源分布，掌握网络的运行状态

C. 根据需求规范和通信规范，实施资源分配和安全规划

D. 理解网络应该具有的功能和性能，设计出符合用户需求的网络

**试题（69）分析**

本题考查网络规划和设计的基础知识。

网络逻辑设计阶段要根据网络用户的分类和分布，选择特定的技术，形成特定的网络结构。网络逻辑结构大致描述了设备的互联及分布情况，但是并不涉及具体的物理位置和运行环境。逻辑设计过程主要由确定逻辑设计目标、网络服务评价、技术选项评价及进行技术决策 4 个步骤组成。

逻辑网络设计工作主要包括网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理和网络安全等内容。

**参考答案**

（69）C

**试题（70）**

利用 SDH 实现广域网互联，如果用户需要的数据传输速率较小，可以用准同步数字系列（PDH）兼容的传输方式在每个 STM-1 帧中封装＿（70）＿个 E1 信道。

（70）A. 4　　B. 63　　C. 255　　D. 1023

**试题（70）分析**

本题考查 SDH 接入的基础知识。

同步数字系列（Synchronous Digital Hierarchy，SDH）是一种将复接、线路传输及

交换功能融为一体的物理传输网络。SDH 不是一种协议，也不是一种传输介质，而是一种传输技术。SDH 网络主要使用光纤通信技术，但也可以使用微波和卫星传送。SDH 可以对网络实现有效的管理、提供实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率，降低网络管理及维护的费用，是运营商主要的基础设施网络。

SDH 采用的信息结构等级称为同步传送模块 STM-N（N=1，4，16，64 等），最基本的模块为 STM-1（155.520Mb/s），4 个 STM-1 同步复用构成 STM-4（622.080Mb/s），16 个 STM-1 同步复用构成 STM-16（2488.320Mb/s）。

如果用户需要的数据传输速率较小，则 SDH 还可以提供准同步数字系列（Plesiochronous Digital Hierarchy，PDH）兼容的传输方式。这种方式在 STM-1 中封装了 63 个 E1 信道，可以同时向 63 个用户提供 2Mb/s 的接入速率。PDH 兼容方式提供两种接口，一是传统的 E1 接口，例如路由器上的 G.703 转 V.35 接口；另一种是封装了多个 E1 信道的 CPOS（Channel POS）接口；路由器通过一个 CPOS 接口接入 SDH 网络，并通过封装的多个 E1 信道连接多个远程站点。

**参考答案**

（70）B

**试题（71）～（75）**

The metric assigned to each network depends on the type of protocol. Some simple protocol, like RIP, treats each network as equals. The __（71）__ of passing through each network is the same; it is one __（72）__ count. So if a packet passes through 10 network to reach the destination, the total cost is 10 hop counts. Other protocols, such as OSPF, allow the administrator to assign a cost for passing through a network based on the type of service required. A __（73）__ through a network can have different costs (metrics). For example, if maximum __（74）__ is the desired type of service, a satellite link has a lower metric than a fiber-optic line. On the other hand, if minimum __（75）__ is the desired type of service, a fiber-optic line has a lower metric than a satellite line. OSPF allow each router to have several routing table based on the required type of service.

（71）A. number B. connection C. diagram D. cost

（72）A. process B. hop C. route D. flow

（73）A. flow B. window C. route D. cost

（74）A. packet B. throughput C. error D. number

（75）A. delay B. stream C. packet D. cost

**参考译文**

赋予每一个网络的路由度量依赖于协议的类型。对于像 RIP 这样的简单协议，可以认为每个网络都是相同的，因而通过每一个网络的费用也都是相同的，其费用为 1。所以，如果一个分组经过 10 个网络到达目标，则总的费用就是 10 跳。其他的协议，例如 OSPF，允许网络管理员根据要求的服务类型赋予所通过的网络一个度量值。通过一个网络的路由可以具有不同的费用。例如，若期望的服务类型为最大吞吐率，则卫星链路比光纤线路的费用低。而如果期望的服务类型为最小延迟，则光纤线路比卫星线路的费用低。OSPF 协议允许每一个路由器根据需要的服务类型设置几个不同的路由表。

**参考答案**

（71）D　（72）B　（73）C　（74）B　（75）A

# 第 8 章　2010 下半年网络工程师下午试题分析与解答

**试题一（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业网拓扑结构如图 1-1 所示。

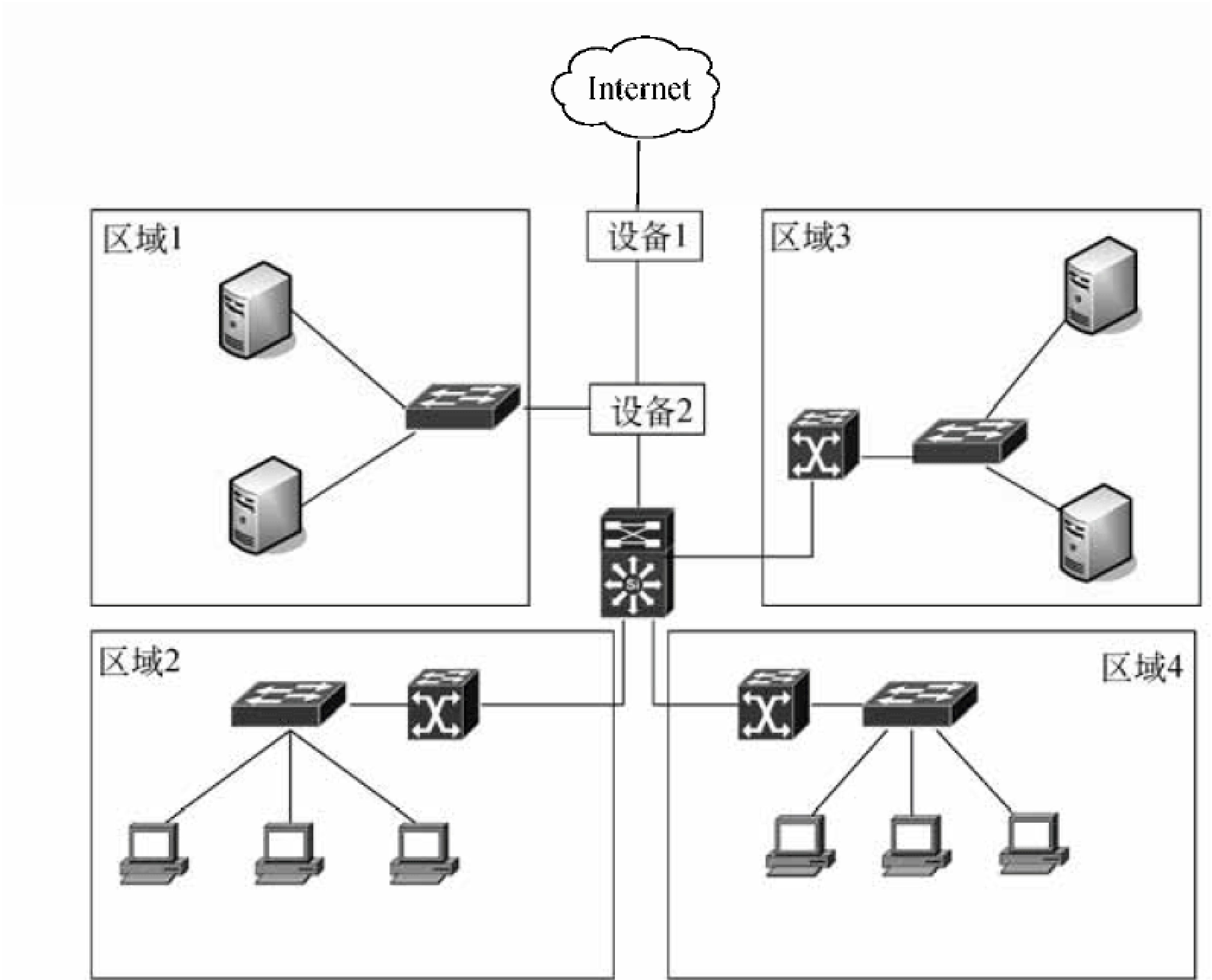



图 1-1

**【问题 1】（4 分）**

企业根据网络需求购置了如下设备，其基本参数如表 1-1 所示。

**表 1-1**

| 设备类型 | 参　　数 |
|---|---|
| A | 模块化接入，固定广域网接口+可选广域网接口，固定局域网接口 100/1000Base-TX |
| B | 背板带宽 1.2Tbps，包转发率 285Mpps，传输速率 10/100/1000Mbps，交换方式：存储转发，应用层级：三层 |

续表

| 设备类型 | 参　数 |
|---|---|
| C | 背板带宽 140Gbps，包转发率 100Mpps，传输速率 10/100Mbps，交换方式：存储转发 |
| D | 24 个固定百兆 RJ45 接口，1 个 GBIC 插槽，包转发率=7.6 Mpps |
| E | 并发连接数 280 000，安全过滤带宽 135Mbps，支持 IDS 及 VPN |

根据网络需求、拓扑图和设备参数类型，图 1-1 中设备 1 应选择类型为__（1）__的设备，设备 2 应选择类型为__（2）__的设备。

**【问题 2】**（4 分）

该网络采用核心层、汇聚层、接入层的三层架构，所有计算机都采用静态 IP 地址。为了防止恶意用户盗用 IP 地址，网管员可采用__（3）__的策略来防止 IP 地址盗用，该策略应在三层架构中的__（4）__层实施。

企业架设 Web 服务器对外进行公司及产品宣传，同时企业内部需架设数据库服务器存放商业机密数据，则 Web 服务器应放置在图 8-1 中的区域__（5）__，数据库服务器应放置在区域__（6）__。

**【问题 3】**（4 分）

若网络管理员决定在企业内部增加 WLAN 接入功能，无线路由器基本参数设置如图 1-2 所示。



图 1-2

网络管理员决定在无线 AP 上开启 MAC 地址过滤功能，若该 AP 的 MAC 地址过滤表如图 1-3 所示，则下面说法正确的是__（7）__。

A. MAC 地址为“00-0A-EB-00-07-5F”的主机可以访问 AP

B. MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“1234567890”来访问 AP

C. MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“0987654321”来访问 AP

D. 其他主机均可以访问本无线网络 AP

若将 MAC 地址过滤规则设为“允许列表中生效规则之外的 MAC 地址访问本无线网络”，则下面说法正确的是__（8）__。

A. MAC 地址为“00-0A-EB-00-07-5F”的主机可以访问 AP

B. MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，不需要输入 WEP 密码

C. MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，需使用 64 位 WEP 密码“1234567890”

D. MAC 地址为“00-0A-EB-00-07-8A”的主机可以访问 AP，不需要输入 WEP 密码

无线网络MAC地址过滤设置

本页设置MAC地址过滤来控制计算机对本无线网络的访问。

**注意：** 64位密钥、128位密钥和152位密钥（16进制形式）只有在安全认证方式为开放系统、共享密钥或自动选择而且设置默认密钥时才有效（否则视为允许通过）。

MAC地址过滤功能：　**已开启**　[关闭过滤]

过滤规则
- ○ 允许列表中生效规则之外的MAC地址访问本无线网络
- ◉ 禁止列表中生效规则之外的MAC地址访问本无线网络

显示内容：
- ○ 描述
- ◉ 密钥

| ID | MAC地址 | 状态/类型 | 密钥 | 编 辑 |
|---|---|---|---|---|
| 1 | 00-0A-EB-00-07-BE | 允许 | | 修改 删除 |
| 2 | 00-0A-EB-00-07-5F | 禁止 | | 修改 删除 |
| 3 | 00-0A-EB-00-07-8A | 64位密钥 | 0987654321 | 修改 删除 |

[添加新条目] [所有条目生效] [所有条目失效] [删除所有条目]

[上一页] [下一页] [帮 助]

图 1-3

**【问题 4】（3 分）**

若 MAC 地址过滤规则如图 1-4 所示，MAC 地址为“00-0A-EB-00-07-5F”的主机能

访问该 AP 吗？请说明原因。

无线网络MAC地址过滤设置

本页设置MAC地址过滤来控制计算机对本无线网络的访问。

**注意：** 64位密钥、128位密钥和152位密钥（16进制形式）只有在安全认证方式为开放系统、共享密钥或自动选择而且设置默认密钥时才有效（否则视为允许通过）。

MAC地址过滤功能：　**已开启**　关闭过滤

过滤规则
- ○ 允许列表中生效规则之外的MAC地址访问本无线网络
- ◉ 禁止列表中生效规则之外的MAC地址访问本无线网络

显示内容：
- ○ 描述
- ◉ 密钥

| ID | MAC地址 | 状态/类型 | 密钥 | 编 辑 |
|---|---|---|---|---|

添加新条目　所有条目生效　所有条目失效　删除所有条目

上一页　下一页　帮 助

图 1-4

## 试题一分析

本题考查网络设备选型、网络基本安全配置方法以及 WLAN 接入方式。

**【问题 1】**

本问题主要考查对网络设备选型的了解和应用。从拓扑结构可以看出，设备 1 是路由设备，设备 2 是防火墙设备。

**【问题 2】**

本问题主要考查网络拓扑的三层结构基本概念及网络设备的放置位置。为了防止用户恶意盗用 IP 地址，网络管理人员可采用 IP 地址与 MAC 地址绑定的策略，同时该策略的实施应该在接入层实施。

从拓扑结构可以看出，区域 1 数据可供外部访问，而区域 3 是企业内部区，因此 Web 服务器可放置在区域 1，而数据库应放置在区域 3。

**【问题 3】**

本问题主要考查 WLAN 的基本安全设置，从图中可以看出，MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“0987654321”来访问 AP。而 MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，需使用 64 位 WEP 密码“0123456789”。

**【问题 4】**

本问题主要考查 WLAN 中的 MAC 地址过滤规则的使用方法，由于过滤规则为“禁止列表中生效规则之外的 MAC 地址访问本无线网络”，过滤列表中又没有任何生效的条目，所以任何主机都不能访问该无线网络。

## 参考答案

**【问题 1】**

（1）A

（2）E

**【问题 2】**

（3）IP 与 MAC 地址绑定

（4）接入

（5）1

（6）3

**【问题 3】**

（7）C. MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“0987654321”来访问 AP。

（8）C. MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，需使用 64 位 WEP 密码“1234567890”。

**【问题 4】**

不能访问。过滤规则为“禁止列表中生效规则之外的 MAC 地址访问本无线网络”，过滤列表中又没有任何生效的条目，所以任何主机都不能访问该无线网络。

## 试题二（共 15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

在 Linux 操作系统中，TCP/IP 网络可通过若干文本文件及命令进行配置。

**【问题 1】（2 分）**

在 Linux 操作系统下，可通过命令＿（1）＿获得如图 2-1 所示的网络配置参数。

```
eth0      Link encap:Ethernet  HWaddr 00:0C:29:16:7B:51
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe16:7b51/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:6262 (6.1 KiB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3068 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3068 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:236640 (231.0 KiB)  TX bytes:236640 (231.0 KiB)
```

图 2-1

（1）备选答案：

A. netconf　　B. ifconf　　C. netconfig　　D. ifconfig

**【问题 2】（3 分）**

在 Linux 操作系统下，可通过命令__（2）__显示路由信息。若主机所在网络的网关 IP 地址为 192.168.0.254，则可使用命令__（3）__ **add default** __（4）__ **192.168.0.254** 添加网关为默认路由。

（2）备选答案：

A. netstat-nr　　B. ls route　　C. ifconfig　　D. netconfig

（3）备选答案：

A. route　　B. netstat　　C. ifconf　　D. ifconfig

（4）备选答案：

A. gateway　　B. gw　　C. gate　　D. g

**【问题 3】（4 分）**

在 Linux 系统中，DNS 查询文件内容如下所示，该文件的默认存储位置为__（5）__，当用户做 DNS 查询时，首选 DNS 服务器的 IP 地址为__（6）__。

Search domain.test.cn
Nameserver 210.34.0.14
Nameserver 210.34.0.15
Nameserver 210.34.0.16
Nameserver 210.34.0.17

（5）备选答案：

A. /etc/inet.conf　　B. /etc/resolv.conf
C. /etc/inetd.conf　　D. /etc/net.conf

（6）备选答案：

A. 210.34.0.14　　B. 210.34.0.15
C. 210.34.0.16　　D. 210.34.0.17

**【问题 4】（6 分）**

文件/etc/sysconfig/network-scripts/eth0 用于存储网络配置信息，请根据图 2-1 填写下面的空缺信息，完成主机的配置。

```
DEVICE=eth0
HWADDR=__(7)__
ONBOOT=yes
BOOTPROTO=none
NETMASK=__(8)__
IPADDR=__(9)__
```

```
GATEWAY=  (10)
TYPE=Ethernet
...
```

**试题二分析**

本题考查 Linux 操作系统下 TCP/IP 的配置。

**【问题 1】**

本问题考查对 ifconfig 命令的了解程度。

**【问题 2】**

本问题考查路由信息的查看命令和默认路由的添加命令。在 Linux 操作系统下，可通过 netstat -nr 显示路由信息。可以使用 route 命令对路由表进行操作。

**【问题 3】**

本问题考查 DNS 的配置，其中 DNS 查询文件默认存储位置为/etc/resolv.conf，从该文件可以看出，首选 DNS 服务器为 210.34.0.14。

**【问题 4】**

本问题考查对文本方式下网络配置的掌握程度。HWADDR 是 MAC 地址信息，NETMASK 是网络掩码信息，IPADDR 为 IP 地址，GATEWAY 为网关 IP 地址。

**参考答案**

**【问题 1】**

（1）D

**【问题 2】**

（2）A

（3）A

（4）B

**【问题 3】**

（5）B

（6）A

**【问题 4】**

（7）00:0C:29:16:7B:51

（8）255.255.255.0

（9）192.168.0.100

（10）192.168.0.254

**试题三（共 15 分）**

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司采用 Windows Server 2003 操作系统构建了一个企业网站，要求用户输入

https://www.test.com 访问该网站。该服务器同时又配置了 FTP 服务，域名为 ftp.test.com。在 IIS 6.0 安装完成后，网站的属性窗口“主目录”“目录安全性”以及“网站”选项卡分别如图 3-1、图 3-2 和图 3-3 所示。




图 3-1

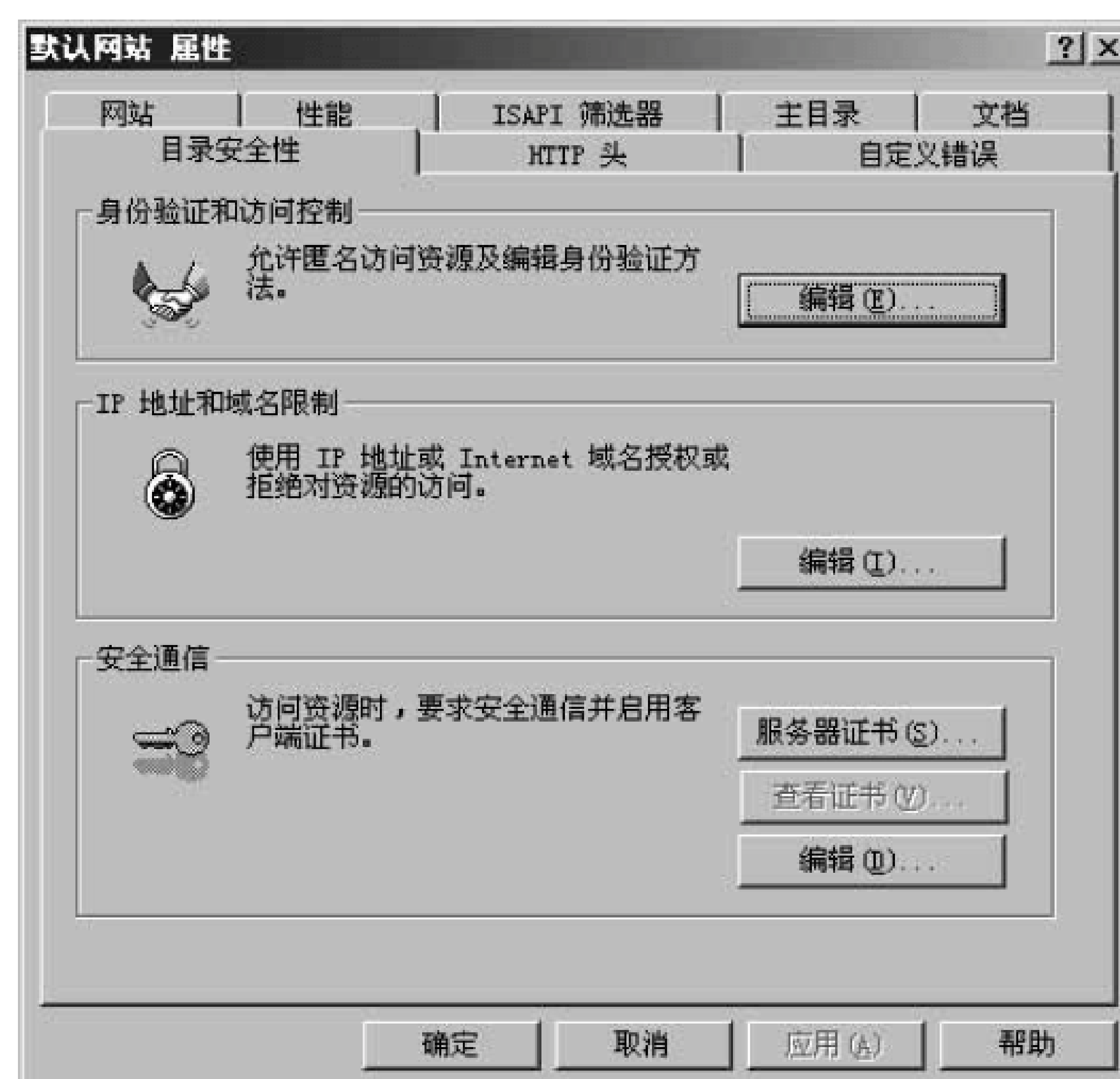



图 3-2

Web 服务器安装完成后，需要在 DNS 服务器中添加记录，为 Web 服务器建立的正向搜索区域记录如图 3-4 所示。

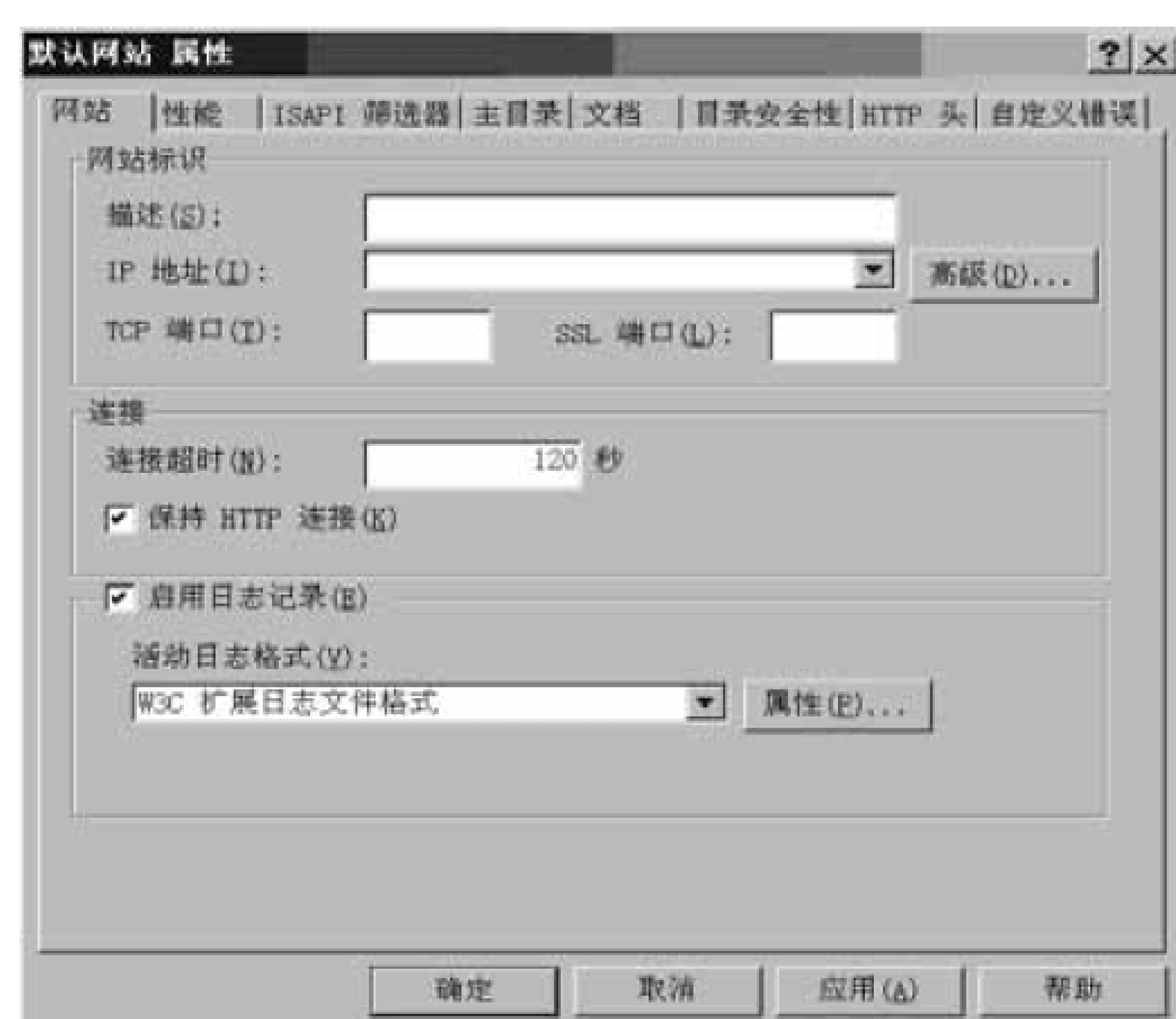



图 3-3

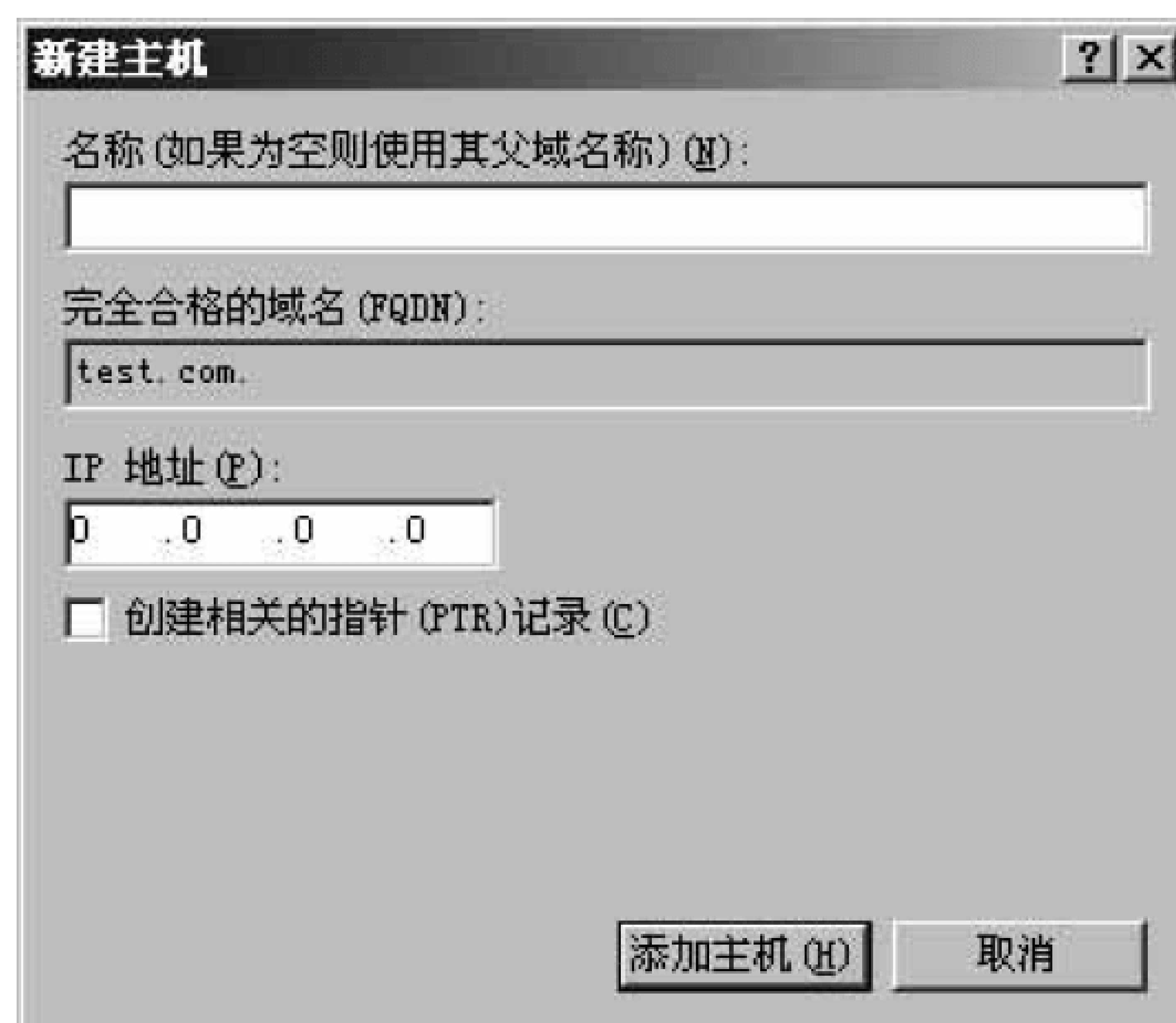



图 3-4

**【问题 1】（2 分）**

为了让用户能够查看网站文件夹中的内容，在图 3-1 中应勾选 ＿（1）＿。

**【问题 2】（3 分）**

为了配置安全的 Web 网站，在图 3-2 中需点击安全通信中的“服务器证书”按钮来获取服务器证书。获取服务器证书共有以下 4 个步骤，正确的排序为 （2） 。

A. 生成证书请求文件

B. 在 IIS 服务器上导入并安装证书

C. 从 CA 导出证书文件

D. CA 颁发证书

**【问题 3】（2 分）**

默认情况下，图 3-3 中“SSL 端口”应填入 （3） 。

**【问题 4】（4 分）**

在图 3-4 中，“名称”栏中应输入 （4） 。

（4）备选答案：

A．https.www　　B．www　　C．https　　D．index

在如图 3-5 所示的下拉菜单中点击 （5） ，可为 ftp.test.com 建立正向搜索区域记录。




图 3-5

**【问题 5】（4 分）**

该 DNS 服务器配置的记录如图 3-6 所示。




图 3-6

邮件交换器中优先级别最高的是__（6）__；

（6）A．[10]mail.abc.com　　B．[8]mail.aaa.com

C．[6]mail.test.com　　D．[2]mail2.test.com

在客户端可以通过__（7）__来测试到 Web 网站的连通性。

（7）A．ping 62.35.216.12　　B．ping 62.35.216.7

C．ping mail.test.com　　D．ping ns7.test.com

**试题三分析**

本题考查在 Windows Server 2003 操作系统中 Web 站点和 DNS 站点的构建与配置，属于常规考点，要求考生细心分析题目中所描述的内容。

**【问题 1】**

在“主目录”选项卡中，有“脚本资源访问”“读取”“写入”“目录浏览”“记录访问”“索引资源”等选项，其中“脚本资源访问”选项允许用户读取网站的脚本原文件，“读取”选项允许用户访问网站资源，“写入”选项允许的权限实际上是对 HTTP PUT 指令的处理，对于普通网站，一般情况下这个权限是不打开的。“目录浏览”则允许用户能够查看网站文件夹中的内容，故正确答案为勾选“目录浏览”。

**【问题 2】**

服务器证书的获取过程通常是先在本地生成证书文件，提交后由 CA 颁发证书，收到证书文件后从 CA 导出文件，最后在 IIS 服务器上导入并安装证书。

**【问题 3】**

SSL 的默认端口为 443。

**【问题 4】**

DNS 记录中，www.test.com 的主机名为 www，故“名称”栏中应输入 www，选 B。采用“新建主机”或“新建别名”均能为 ftp.test.com 建立正向搜索区域记录。

**【问题 5】**

邮件交换器中优先级别最高的是[2]mail2.test.com。从图 3-6 中可以看出，62.35.216.7 同时配置了 Web 和 ftp 服务，故可采用 ping 62.35.216.7 命令来测试到 Web 网站的连通性。

**参考答案**

**【问题 1】**

（1）“目录浏览”

**【问题 2】**

（2）ADCB

**【问题 3】**

（3）443

**【问题 4】**

（4）B．www

（5）新建主机 或 新建别名

**【问题 5】**

（6）D．[2]mail2.test.com

（7）B．ping 62.35.216.7

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业在公司总部和分部之间采用两台 Windows Server 2003 服务器部署企业 IPSec VPN，将总部和分部的两个子网通过 Internet 互联，如图 4-1 所示。

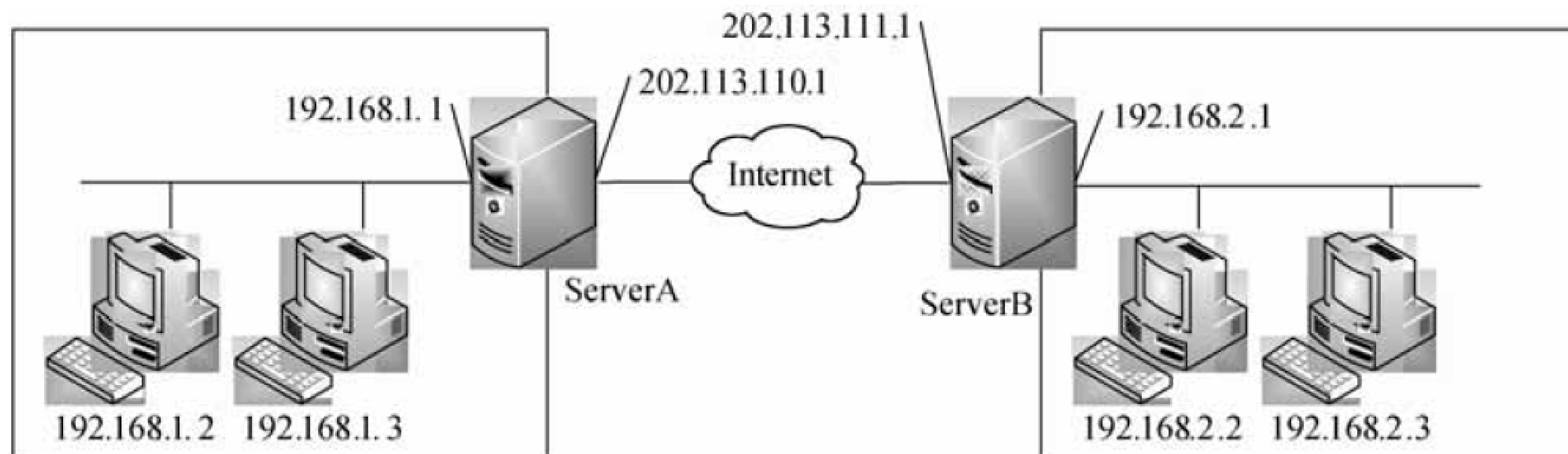



图 4-1

【问题 1】（3 分）

隧道技术是 VPN 的基本技术，隧道是由隧道协议形成的，常见隧道协议有 IPSec、PPTP 和 L2TP，其中＿（1）＿和＿（2）＿属于第二层隧道协议，＿（3）＿属于第三层隧道协议。

【问题 2】（3 分）

IPSec 安全体系结构包括 AH、ESP 和 ISA KMP/Oakley 等协议。其中，＿（4）＿为 IP 包提供信息源验证和报文完整性验证，但不支持加密服务；＿（5）＿提供加密服务；＿（6）＿提供密钥管理服务。

【问题 3】（6 分）

设置 ServerA 和 ServerB 之间通信的筛选器属性界面如图 4-2 所示，在 ServerA 的 IPSec 安全策略配置过程中，当源地址和目标地址均设置为“一个特定的 IP 子网”时，源子网 IP 地址应设为＿（7）＿，目标子网 IP 地址应设为＿（8）＿。图 4-3 所示的隧道设置中的隧道终点 IP 地址应设为＿（9）＿。

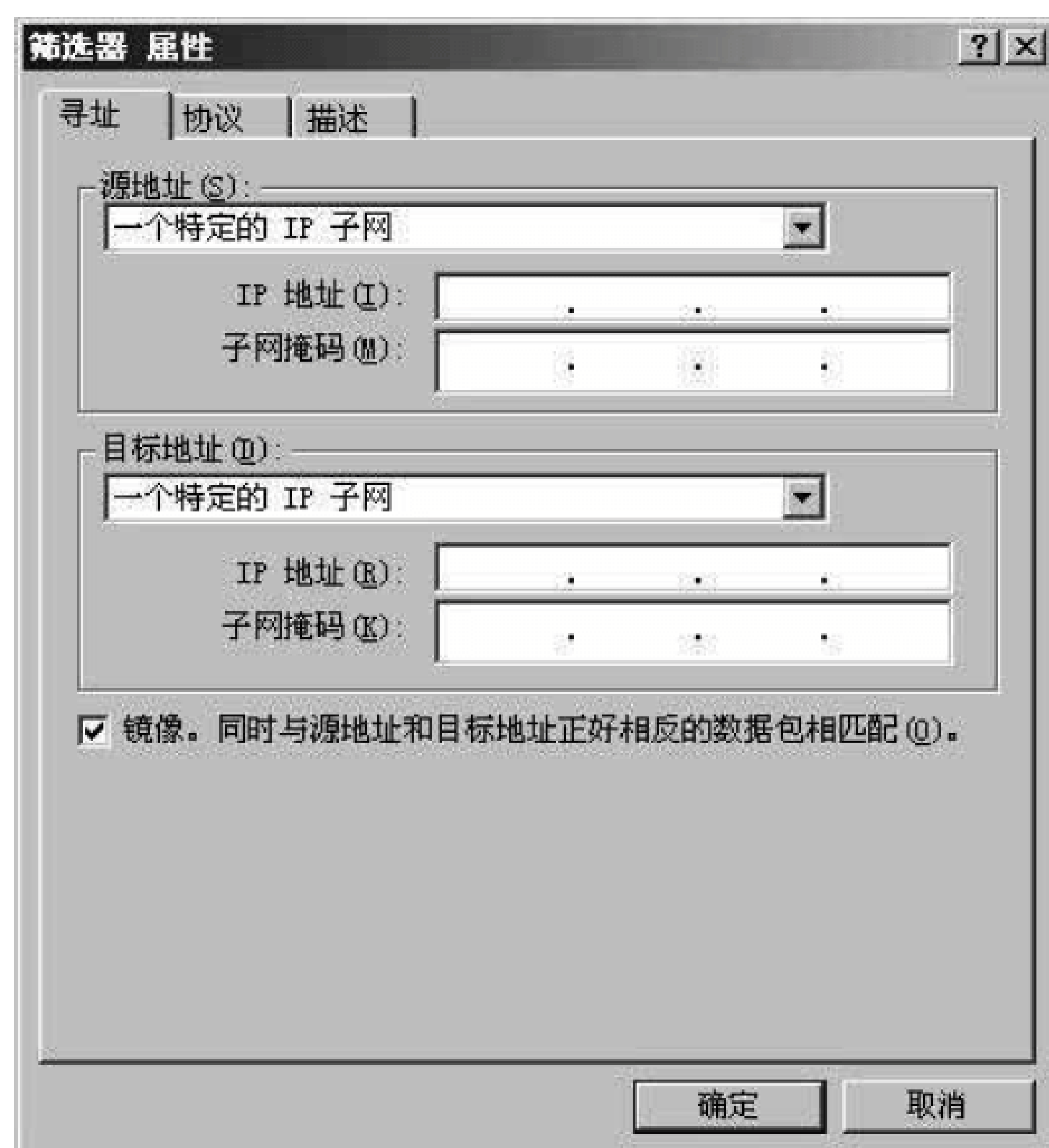



图 4-2

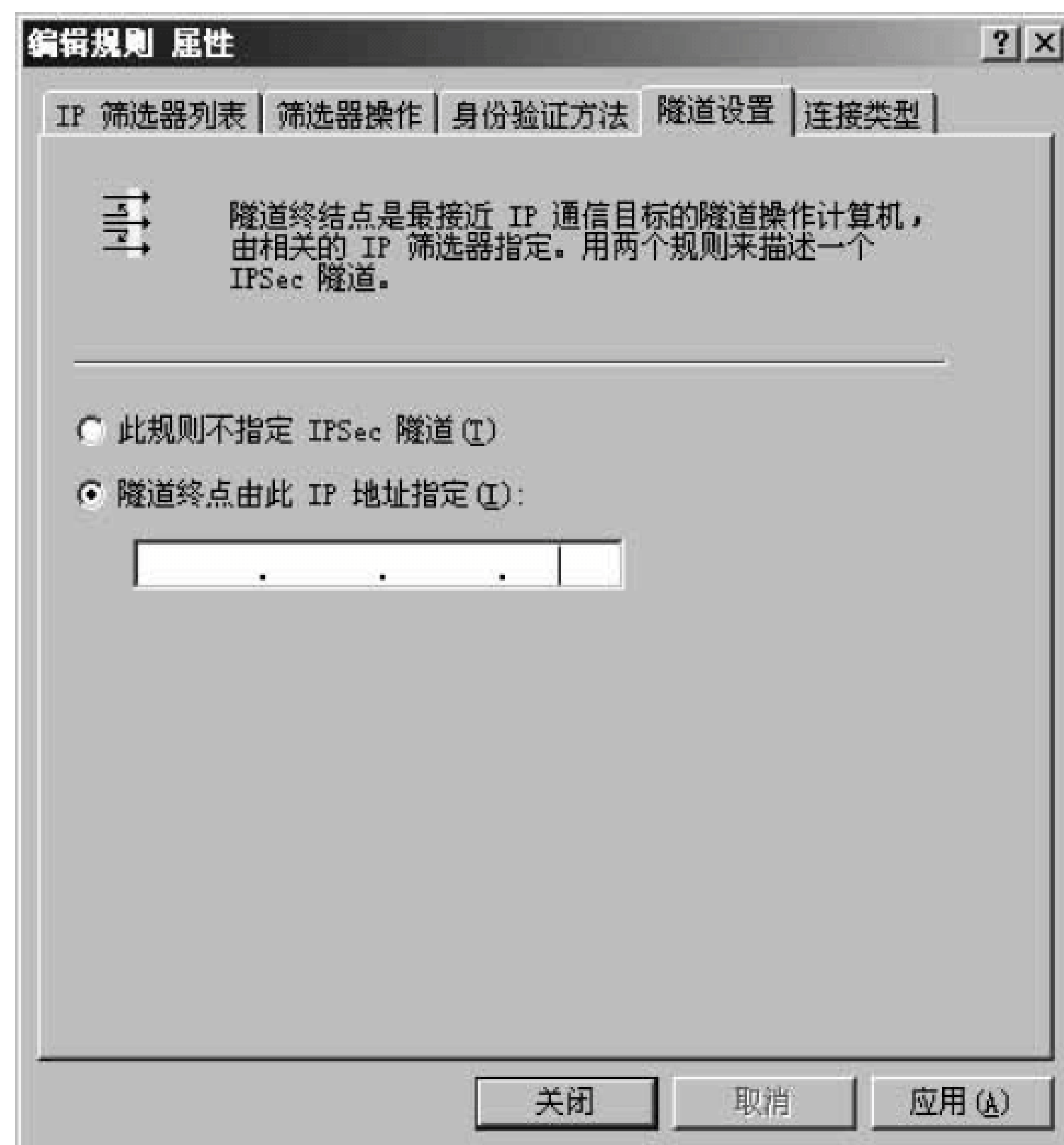



图 4-3

【问题 4】（3 分）

在 ServerA 的 IPSec 安全策略配置过程中，ServerA 和 ServerB 之间通信的 IPSec 筛选器“许可”属性设置为“协商安全”，并且安全措施为“加密并保持完整性”，如图 4-4 所示。根据上述安全策略填写图 4-5 中的空格，表示完整的 IPSec 数据包格式。

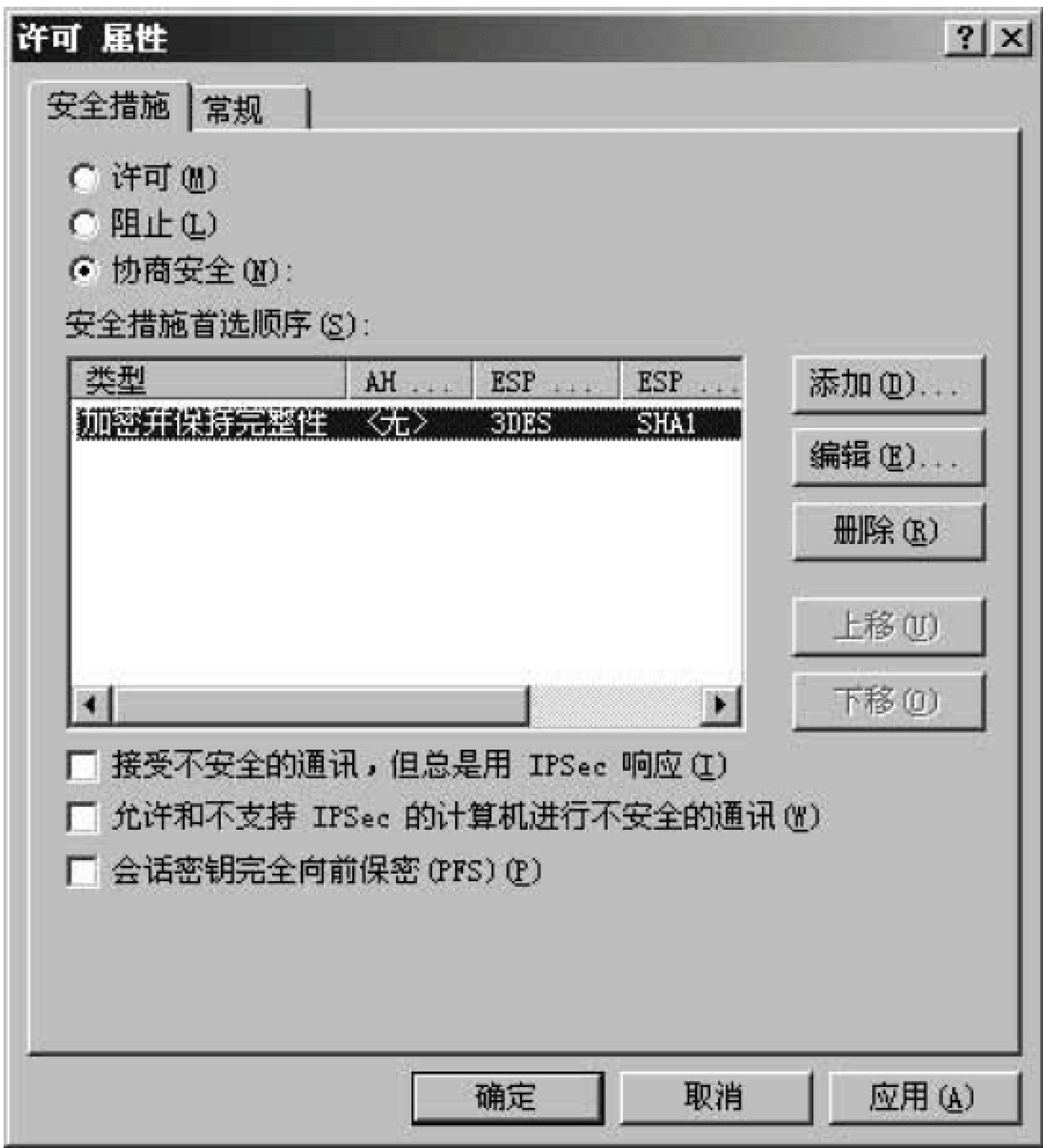



图 4-4

| 新 IP 头 | （10） | （11） | TCP 头 | 数据 | （12） |
|---|---|---|---|---|---|

图 4-5

（10）～（12）备选答案：

A．AH 头　　B．ESP 头　　C．旧 IP 头　　D．新 TCP 头

E．AH 尾　　F．ESP 尾　　G．旧 IP 尾　　H．新 TCP 尾

**试题四分析**

本题考查 IPSec 相关知识点，包括 IPSec 基础知识和 Windows 系统中 IPSec 安全策略配置两部分内容。

**【问题 1】**

本问题考查 VPN 隧道技术的基本概念。

隧道技术是 VPN 的基本技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。L2TP 协议是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。

【问题 2】

本问题考查 IPSec 的基本概念。

IPSec 安全体系结构包括 AH、ESP 和 ISAKMP/Oakley 等协议。IPSec 认证头提供了数据完整性和数据源认证，但是不提供保密服务。AH 包含了对称密钥的散列函数，使得第三方无法修改传输中的数据。IPSec 封装安全负荷（ESP）提供了数据加密功能。ESP 利用对称密钥对 IP 数据（例如 TCP 包）进行加密。IPSec 传送认证或加密的数据之前，必须就协议、加密算法和使用的密钥进行协商。密钥交换协议 IKE 提供这个功能，并且在密钥交换之前还要对远程系统进行初始的认证。IKE 实际上是 3 个协议 ISAKMP（Internet Security Association and Key Management Protocol）、Oakley 和 SKEME（Versatile Secure Key Exchange Mechanism for Internet protocol）的混合体。

【问题 3】

本问题考查 Windows 中 IPSec 的配置。

在 ServerA 上配置 IPSec 的过程中，筛选器的源子网地址应该是 ServerA 连接的内部子网 192.168.1.1/32，目标子网地址应该是 ServerB 连接的内部子网 192.168.1.2/32，在图 4-2 中用源 IP 地址 1921.68.1.0 代表源子网，目标 IP 地址 192.168.2.0 代表目标子网。图 4-3 中的隧道终点 IP 地址应设为 ServerB 的入口地址 202.113.111.1。

【问题 4】

本问题考查 IPSec 的综合知识。

在 ServerA 的 IPSec 安全策略配置过程中，ServerA 和 ServerB 之间通信的 IPSec 筛选器"许可"属性设置为"协商安全"，并且安全措施为"加密并保持完整性"，而支持"加密并保持完整性"提示了 ServerA 和 ServerB 之间的 IPSec 通信只能采用 ESP 协议。而公司总部和分部之间的 VPN 采用隧道模式通信，所以 IPSec 数据包的格式就是 ESP 的隧道模式，该模式的数据包可以表示为下图。

| 新的IP头 | ESP头 | 原来的IP头 | TCP | 数据 | ESP尾 |
|---|---|---|---|---|---|

## 参考答案

【问题 1】

（1）PPTP

（2）L2TP（（1）、（2）顺序可调换）

（3）IPSec

【问题 2】

（4）AH

（5）ESP

（6）ISAKMP/Oakley

【问题 3】

（7）192.168.1.0

（8）192.168.2.0

（9）202.113.111.1

【问题 4】

（10）B 或 ESP 头

（11）C 或旧 IP 头

（12）F 或 ESP 尾

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某单位的两个分支机构各有 1 台采用 IPv6 的主机，计划采用 IPv6-over-IPv4 GRE 隧道技术实现两个分支机构的 IPv6 主机通信，其网络拓扑结构如图 5-1 所示。

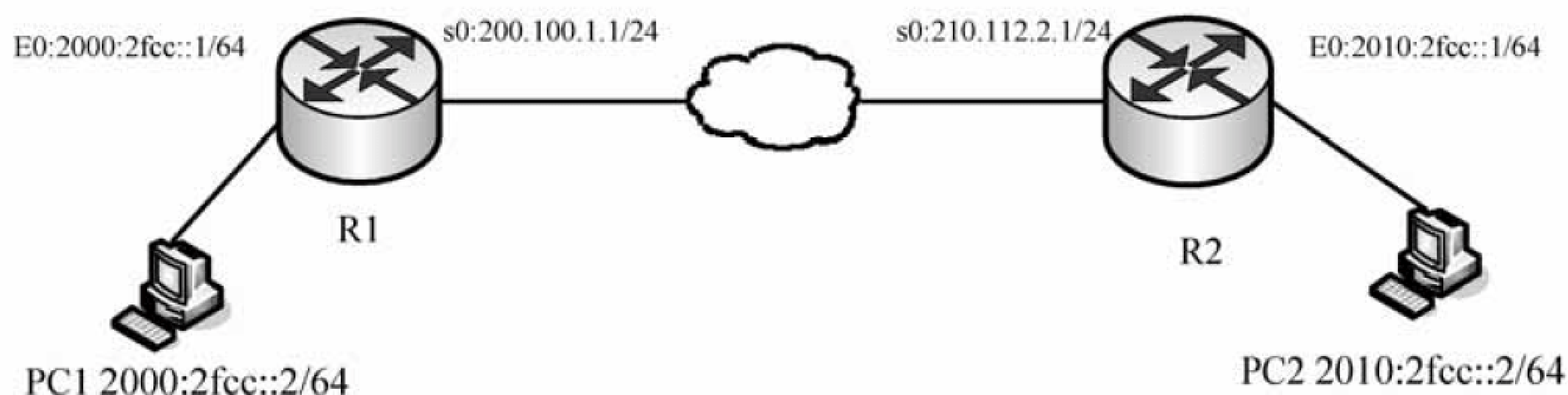



图 5-1

【问题 1】（2 分）

使用 IPv6-over-IPv4 GRE 隧道技术，可在 IPv4 的 GRE 隧道上承载 IPv6 数据报文。此时__（1）__作为乘客协议，__（2）__作为承载协议。

【问题 2】（6 分）

根据网络拓扑和需求说明，完成（或解释）路由器 R1 的配置。

```
Router(config)# ipv6 unicast-routing                    （3）
R1(config)# interface Serial 1/0
R1(config-if)# （4） address （5） （6）          （设置串口地址）
R1(config-if)#no shutdown                         （开启串口）
R1(config)#interface FastEthernet0/0
R1(config-if)# （7）address （8）                （设置以太口地址）
R1(config-if)#exit
```

【问题 3】（6 分）

根据网络拓扑和需求说明，解释路由器 R2 的 GRE 隧道配置。

```
…
R2(config)#interface tunnel 0                  （启用 tunnel 0）
R2(config-if)#tunnel source s1/0                （9）
R2(config-if)#tunnel destination 200.100.1.1    （10）
R2(config-if)#ipv6 address 2000:2fcc::2/64     （为 tunnel 配置 IPv6 地址）
R2(config-if)#tunnel mode gre ipv6              （11）
```

**【问题 4】（1 分）**

IPv6 主机 PC1 的 IP 地址为 2000:2fcc::2/64，在这种配置环境下，其网关地址应为（12）。

**试题五分析**

本题考查 IPv6-over-IPv4 GRE 隧道配置的知识。

**【问题 1】**

本问题考查 IPv6-over-IPv4 GRE 隧道的基本概念。

IPv6-over-IPv4 隧道是将 IPv6 报文封装在 IPv4 报文中，让 IPv6 数据包穿过 IPv4 网络进行通信。对于采用隧道技术的设备来说，在隧道的入口处，将 IPv6 的数据报封装进 IPv4，IPv4 报文的源地址和目的地址分别是隧道入口和隧道出口的 IPv4 地址；在隧道的出口处，再将 IPv6 报文取出转发到目的节点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，容易实现。但是，隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

使用标准的 GRE 隧道技术，可在 IPv4 的 GRE 隧道上承载 IPv6 数据报文。GRE 隧道是两点之间的连路，每条连路都是一条单独的隧道。GRE 隧道把 IPv6 作为乘客协议，将 GRE 作为承载协议。所配置的 IPv6 地址是在 Tunnel 接口上配置的，而所配置的 IPv4 地址是 Tunnel 的源地址和目的地址（隧道的起点和终点）。

**【问题 2】**

本问题考查路由器接口地址的基本配置操作。

根据题目的拓扑结构图可知，路由器 R1 的 S0 口地址为：200.100.1.1/24；E0 口地址为：2000:2fcc::1/64，所以配置命令如下。

```
Router(config)# ipv6 unicast-routing                       (开启 IPv6 单播路由)
R1(config)# interface Serial 1/0
R1(config-if)# ip address 200.100.1.1 255.255.255.0  （设置串口地址）
R1(config-if)#no shutdown                                  （开启串口）
R1(config)#interface FastEthernet0/0
R1(config-if)# IPv6 address 2000:2fcc::1/64                （设置以太口地址）
R1(config-if)#exit
```

**【问题 3】**

本问题考查 GRE 隧道基本配置操作。

根据网络拓扑和需求说明，路由器 R2 的 GRE 隧道配置如下：

```
…
R2(config)#interface tunnel 0                  (启用 tunnel 0)
R2(config-if)#tunnel source s1/0               (指定隧道(tunnel)的源为 S0)
R2(config-if)#tunnel destination 200.100.1.1 (指定隧道(tunnel)的目标地址)
R2(config-if)#ipv6 address 2000:2fcc::2/64   (为 tunnel 配置 IPv6 地址)
R2(config-if)#tunnel mode gre ipv6            (tunnel 模式为 IPv6 的 GRE 隧道)
```

**【问题 4】**

本问题考查使用 IPv6-over-IPv4 GRE 隧道时，使用 IPv6 的 PC 上的基本配置操作。

IPv6 主机 PC1 的 IP 地址为 2000:2fcc::2/64，根据网络拓扑图可知，其网关地址应为路由器 R1 的 E0 口地址 2000:2fcc::1/64。

**参考答案**

**【问题 1】**

（1）IPv6

（2）IPv4 GRE

**【问题 2】**

（3）开启 IPv6 单播路由

（4）ip

（5）200.100.1.1

（6）255.255.255.0

（7）IPv6

（8）2000:2fcc::1/64

**【问题 3】**

（9）指定隧道（tunnel）的源为 S0

（10）指定隧道（tunnel）的目标地址

（11）tunnel 模式为 IPv6 的 GRE 隧道

**【问题 4】**

（12）2000:2fcc::1/64

# 第 9 章　2011 上半年网络工程师上午试题分析与解答

**试题（1）**

在 CPU 中用于跟踪指令地址的寄存器是__（1）__。

（1）A．地址寄存器（MAR）　　B．数据寄存器（MDR）
　　C．程序计数器（PC）　　D．指令寄存器（IR）

**试题（1）分析**

本题考查寄存器的基本知识。

CPU 中通常设置一些寄存器，用于暂时存储程序运行过程中的相关信息。其中，通用寄存器常用于暂存运算器需要的数据或运算结果，地址寄存器和数据寄存器用于访问内存时的地址和数据暂存，指令寄存器用于暂存正在执行的指令，程序计数器中存放待执行的指令的地址。

**参考答案**

（1）C

**试题（2）**

指令系统中采用不同寻址方式的目的是__（2）__。

（2）A．提高从内存获取数据的速度　　B．提高从外存获取数据的速度
　　C．降低操作码的译码难度　　D．扩大寻址空间并提高编程灵活性

**试题（2）分析**

本题考查指令系统的基本概念。

寻址方式是指寻找操作数或操作数地址的方式。指令系统中采用不同寻址方式的目的是为了在效率和方便性上找一个平衡。立即数寻址和寄存器寻址在效率上是最快的，但是寄存器数目少，不可能将操作数都存入其中等待使用，立即数的使用场合也非常有限，这样就需要将数据保存在内存中，然后使用直接寻址、寄存器间接寻址、寄存器相对寻址、基址加变址寻址、相对基址加变址寻址这些寻址方式将内存中的数据移入寄存器中。

**参考答案**

（2）D

**试题（3）**

在计算机系统中采用总线结构，便于实现系统的积木化构造，同时可以__（3）__。

（3）A．提高数据传输速度　　B．提高数据传输量
　　C．减少信息传输线的数量　　D．减少指令系统的复杂性

**试题（3）分析**

本题考查计算机系统的基础知识。

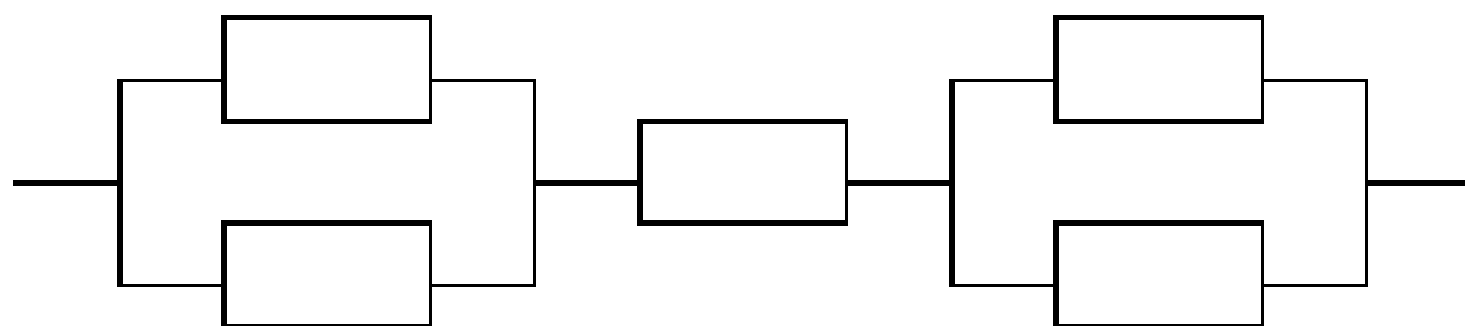
总线是连接计算机有关部件的一组信号线，是计算机中用来传送信息代码的公共通道。采用总线结构主要有以下优点：简化系统结构，便于系统设计制造；大大减少了连线数目，便于布线，减小体积，提高系统的可靠性；便于接口设计，所有与总线连接的设备均采用类似的接口；便于系统的扩充、更新与灵活配置，易于实现系统的模块化；便于设备的软件设计，所有接口的软件就是对不同的口地址进行操作；便于故障诊断和维修，同时也降低了成本。

**参考答案**

（3）C

**试题（4）**

某计算机系统由下图所示的部件构成，假定每个部件的千小时可靠度都为 $R$，则该系统的千小时可靠度为__（4）__。



（4）A. $R+2R/4$　　B. $R+R^2/4$

C. $R(1-(1-R)^2)$　　D. $R(1-(1-R)^2)^2$

**试题（4）分析**

本题考查系统可靠性方面的基础知识。

由子系统构成串联系统时，其中任何一个子系统失效就足以使系统失效，其可靠度等于各子系统可靠度的乘积；构成并联系统时，只要有一个子系统正常工作，系统就能正常工作。

设每个子系统的可靠性分别以 $R_1, R_2, \cdots, R_N$ 表示，则整个系统用串联方式构造时的可靠度为 $R = R_1 \times R_2 \cdots \times \cdots R_N$，整个系统用串联方式构造时的可靠度为 $R = 1-(1-R_1)(1-R_2)\cdots(1-R_N)$。

因此，本系统的可靠度为 $R(1-(1-R)^2)^2$。

**参考答案**

（4）D

**试题（5）**

软件产品的可靠性并不取决于__（5）__。

（5）A. 潜在错误的数量　　B. 潜在错误的位置

C. 软件产品的使用方式　　D. 软件产品的开发方式

**试题（5）分析**

本题考查软件质量管理。

软件可靠性指的是一个系统对于给定的时间间隔内、在给定条件下无失效运作的概率。根据定义，软件可靠性与软件的潜在错误的数量、位置有关，与软件产品的使用方式有关，而软件产品的开发方式不决定软件产品的可靠性。

**参考答案**

（5）D

**试题（6）**

模块 A 直接访问模块 B 的内部数据，则模块 A 和模块 B 的耦合类型为__（6）__。

（6）A．数据耦合　　B．标记耦合　　C．公共耦合　　D．内容耦合

**试题（6）分析**

本题考查软件的分析与设计方法。

模块独立性是创建良好设计的一个重要原则，一般采用模块间的耦合和模块的内聚两个准则来进行度量。耦合是模块之间的相对独立性的度量，模块之间的连接越紧密，联系越多，耦合性就越高，而其模块独立性就越弱。一般来说，模块之间的耦合有 7 种类型，根据耦合性从低到高为非直接耦合、数据耦合、标记耦合、控制耦合、外部耦合、公共耦合和内容耦合。如果一个模块访问另一个模块时，彼此之间是通过数据参数（不是控制参数、公共数据结构或外部变量）来交换输入、输出信息的，则称这种耦合为数据耦合；如果一组模块通过数据结构本身传递，则称这种耦合为标记耦合；若一组模块都访问同一个公共数据环境，则它们之间的耦合就称为公共耦合；若一个模块直接访问另一个模块的内部数据、一个模块不通过正常入口转到另一个模块内部、两个模块有一部分程序代码重叠或者一个模块有多个入口，上述几个情形之一发生则两个模块之间就发生了内容耦合。

**参考答案**

（6）D

**试题（7）**

下列关于风险的叙述不正确的是：风险是指__（7）__。

（7）A．可能发生的事件　　B．一定会发生的事件
　　C．会带来损失的事件　　D．可能对其进行干预，以减少损失的事件

**试题（7）分析**

本题考查风险分析和风险控制技术。

风险是一种具有负面后果的、人们不希望发生的事件。通常认为风险具有以下特点：风险是可能发生的事件，其发生的可能性用风险概率来描述；风险是会给项目带来损失的时间；可能对风险进行干预，以期减少损失。针对每一种风险，应弄清可能减少造成损失或避免损失的程度。对风险加以控制，采取一些有效的措施来降低风险或是消除

风险。

**参考答案**

（7）B

**试题（8）**

下列关于项目估算方法的叙述不正确的是__（8）__。

（8）A．专家判断方法受到专家经验和主观性影响

B．启发式方法（如 COCOMO 模型）的参数难以确定

C．机器学习方法难以描述训练数据的特征和确定其相似性

D．结合上述三种方法可以得到精确的估算结果

**试题（8）分析**

本题考查项目管理及工具技术。

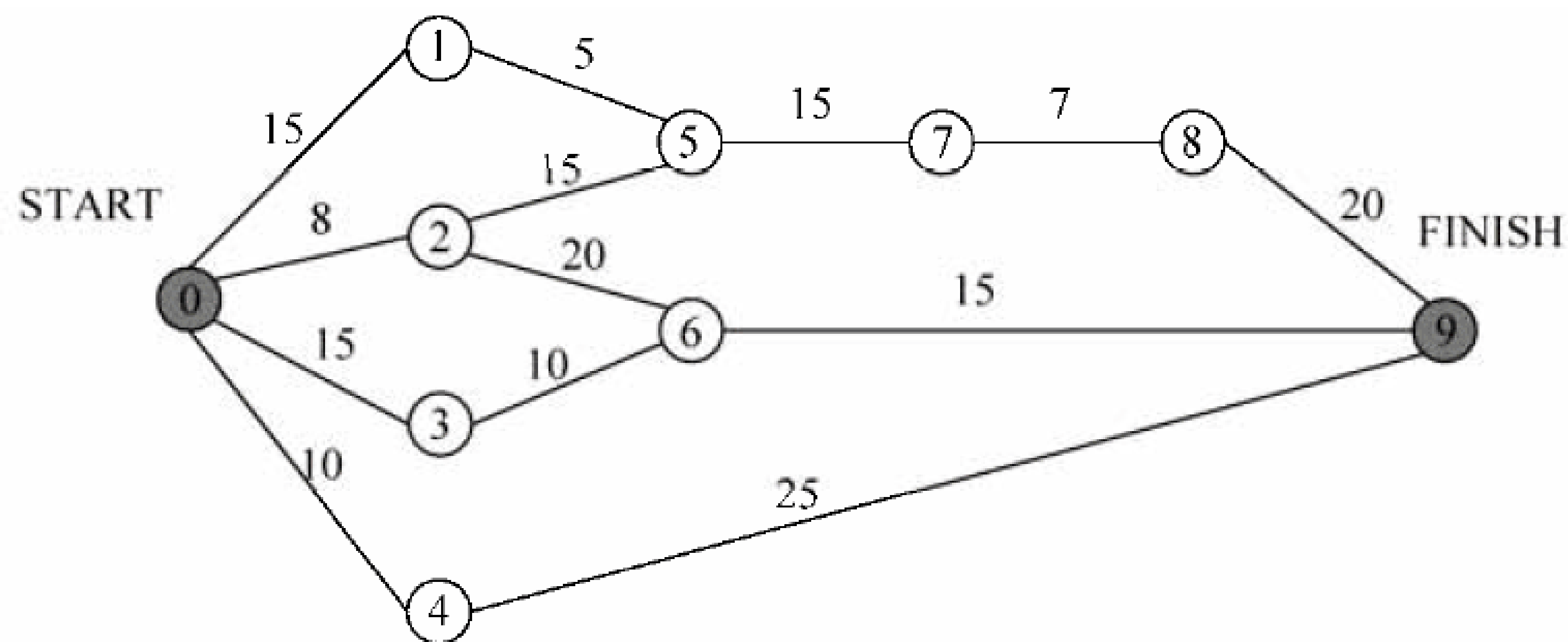
项目估算是项目计划和管理的一个至关重要的方面。成本超出某个限度可能导致客户取消项目，而过低的成本估算可能会迫使开发小组投入大量的时间却没有相应的经济回报。目前常用的项目估算方法有专家判断方法，该方法受到专家经验和主观性等方面的影响；算法方法，根据某个计算模型来估算项目开发成本，如启发式方法 COCOMO 模型，但这些模型中的参数难以确定；机器学习方法，如根据过去的项目开发数据，建立分类模型，预测新项目的开发成本，但这类方法中难以定义训练数据的特征以及定义数据对象之间的相似性。即使结合多种方法，上述问题仍然存在，因此并不能得到精确地估算结果。

**参考答案**

（8）D

**试题（9）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，边表示包含的活动，边上的权重表示活动的持续时间，则里程碑__（9）__在关键路径上。




（9）A．1　　B．2　　C．3　　D．4

**试题（9）分析**

本题考查项目管理及工具技术。

根据关键路径法，计算出关键路径为 0—2—5—7—8—9，关键路径长度为 65。因此里程碑 2 在关键路径上，而里程碑 1、3 和 4 不在关键路径上。

**参考答案**

（9）B

**试题（10）**

下列关于软件著作权中翻译权的叙述不正确的是：翻译权是指＿（10）＿的权利。

（10）A．将原软件从一种自然语言文字转换成另一种自然语言文字
　　B．将原软件从一种程序设计语言转换成另一种程序设计语言
　　C．软件著作权人对其软件享有的以其他各种语言文字形式再表现
　　D．对软件的操作界面或者程序中涉及的语言文字翻译成另一种语言文字

**试题（10）分析**

软件著作权中翻译权是指以不同于原软件作品的一种程序语言转换该作品原使用的程序语言，而重现软件作品内容的创作的产品权利。简单地说，也就是指将原软件从一种程序语言转换成另一种程序语言的权利。

**参考答案**

（10）B

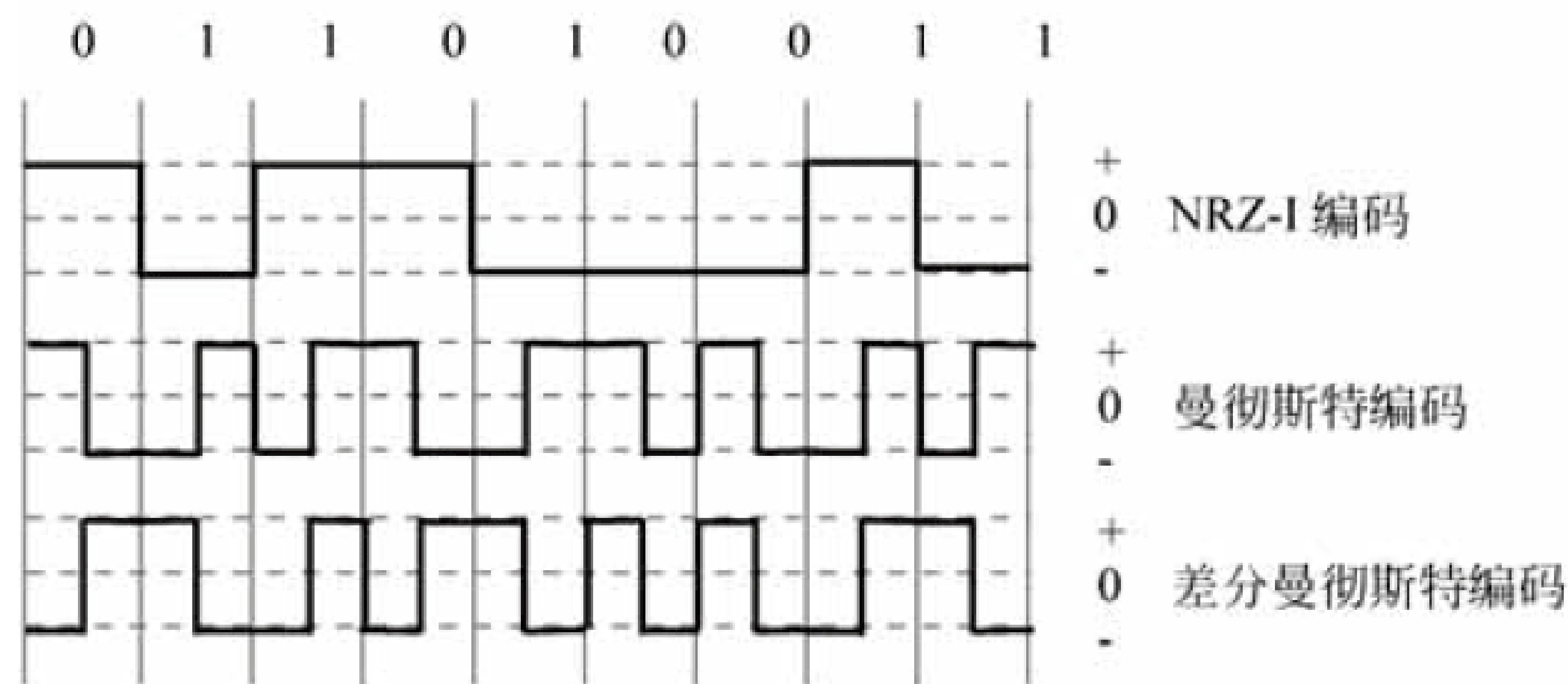
**试题（11）、（12）**

10Base-T 以太网使用曼彻斯特编码，其编码效率为＿（11）＿%，在快速以太网中使用 4B/5B 编码，其编码效率为＿（12）＿%。

（11）A．30　　B．50　　C．80　　D．90
（12）A．30　　B．50　　C．80　　D．90

**试题（11）、（12）分析**

曼彻斯特编码和差分曼彻斯特编码都是双相码，即码元取正负两个不同的电平，或者说由正负两个不同的码元表示一个比特，如下图所示。这种编码的效率就是 50%，但是由于每个比特中间都有电平跳变，因而提供了丰富的同步信息。这两种编码使用在数据速率不太高的以太网中。




为了提高编码的效率，降低电路成本，可以采用 4B/5B 编码，其原理如下图所示。




这实际上是一种两级编码方案。系统中使用不归零码（NRZ），在发送到传输介质之前要变成见 1 就翻不归零码（NRZ-I）。NRZ-I 代码序列中 1 的个数越多，越能提供同步定时信息，但如果遇到长串的 0，则不能提供同步信息。所以在发送到介质上之前还需经过一次 4B/5B 编码，发送器扫描要发送的比特序列，4 位分为一组，然后按照下表的对应规则变换成 5 位的代码。

| 十六进制数 | 4 位二进制数 | 4B/5B 码 | 十六进制数 | 4 位二进制数 | 4B/5B 码 |
|---|---|---|---|---|---|
| 0 | 0000 | 11110 | 8 | 1000 | 10010 |
| 1 | 0001 | 01001 | 9 | 1001 | 10011 |
| 2 | 0010 | 10100 | A | 1010 | 10110 |
| 3 | 0011 | 10101 | B | 1011 | 10111 |
| 4 | 0100 | 01010 | C | 1100 | 11010 |
| 5 | 0101 | 01011 | D | 1101 | 11011 |
| 6 | 0110 | 01110 | E | 1110 | 11100 |
| 7 | 0111 | 01111 | F | 1111 | 11101 |

5 位二进制代码的状态共有 32 种，在上表选用的 5 位代码中 1 的个数都不小于 2 个。这就保证了在介质上传输的代码能提供足够多的同步信息。另外，还有 8B/10B 等编码方法，其原理是类似的。这两种编码的效率是 80%

**参考答案**

（11）B　（12）C

**试题（13）**

在相隔 400km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发送到接收完数据需要的时间是__（13）__。

（13）A．480ms　　B．607ms　　C．612ms　　D．627ms

**试题（13）分析**

一个数据包从开始发送到接收完成的时间包含两部分：发送时间 $t_f$ 和传播延迟时间 $t_p$，根据题目要求可以计算如下。

对电缆信道：$t_p$=400km/(200km/ms)=2ms，$t_f$=3000bit/4800b/s=625ms，$t_p+t_f$=627ms。

**参考答案**

（13）D

**试题（14）**

假设模拟信号的最高频率为 10MHz，采样频率必须大于__（14）__时，才能使得到的

样本信号不失真。

（14）A．6MHz　　B．12MHz　　C．18MHz　　D．20MHz

**试题（14）分析**

模拟信号通过数字信道传输具有效率高、失真小的优点，而且可以开发新的通信业务。常用的数字化技术就是脉冲编码调制技术（Pulse Code Modulation，PCM），简称脉码调制。PCM 主要经过 3 个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变换为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组输出。

采样的频率决定了恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

$$f = \frac{1}{T} \geqslant 2f_{\max}$$

其中，$f$ 为采样频率，$T$ 为采样周期，$f_{\max}$ 为信号的最高频率。

根据题意，对于最高频率为 10MHz 的模拟信号，采样频率必须大于 20MHz。

**参考答案**

（14）D

**试题（15）**

数据链路协议 HDLC 是一种__（15）__。

（15）A．面向比特的同步链路控制协议　　B．面向字节计数的同步链路控制协议

C．面向字符的同步链路控制协议　　D．异步链路控制协议

**试题（15）分析**

数据链路控制协议可分为两大类：面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，并用 10 个专用字符（例如 STX、ETX、ACK、NAK 等）控制传输过程，这类协议发展较早，至今仍在使用。面向比特的协议以比特作为传输的基本单位，它的传输效率高，广泛应用于公用数据网中。

HDLC 协议的全称是高级数据链路控制协议（High Level Data Link Control），在数据链路两端的对等实体之间实现同步控制传输。

**参考答案**

（15）A

**试题（16）**

快速以太网标准 100Base-TX 规定的传输介质是__（16）__。

（16）A．2 类 UTP　　B．3 类 UTP

C．5 类 UTP　　D．光纤

**试题（16）分析**

1995 年 100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为 62.5μm，包层直径为 125μm，单模光线芯线直径为 8μm，包层直径也是 125μm。

| 标　准 | 传 输 介 质 | 特 性 阻 抗 | 最 大 段 长 |
|---|---|---|---|
| 100BASE-TX | 2 对 5 类 UTP | 100Ω | 100m |
| | 2 对 STP | 150Ω | |
| 100BASE-FX | 一对多模光纤 MMF | 62.5/125μm | 2km |
| | 一对单模光纤 SMF | 8/125μm | 40km |
| 100BASE-T4 | 4 对 3 类 UTP | 100Ω | 100m |
| 100BASE-T2 | 2 对 3 类 UTP | 100Ω | 100m |

**参考答案**

（16）C

**试题（17）**

以太网交换机的交换方式有三种，这三种交换方式不包括__（17）__。

（17）A. 存储转发式交换　　B. IP 交换

C. 直通式交换　　D. 碎片过滤式交换

**试题（17）分析**

以太网交换机的交换方式分为存储转发式交换、直通式交换和碎片过滤式交换三类。

① 存储转发式交换（Store and Forward）：交换机对输入的数据包先进行缓存、验证、碎片过滤，然后再进行转发。这种交换方式延时大，但是可以提供差错校验，并支持不同速度的输入/输出端口间的交换（非对称交换），是交换机的主流工作方式。

② 直通式交换（Cut-through）：直通式交换类似于采用交叉矩阵的电话交换机，它在输入端口扫描到目标地址后立即开始转发。这种交换方式的优点是延迟小、交换速度快。其缺点是没有检错能力；不能实现非对称交换；并且当交换机的端口增加时，交换矩阵实现起来比较困难。

③ 碎片过滤式交换（Fragment Free）：这是介于直通式和存储转发式之间的一种解决方案。交换机在开始转发前先检查数据包的长度是否够 64 个字节，如果小于 64 字节，说明是冲突碎片，则丢弃之；如果大于等于 64 字节，则转发该包。这种转发方式的处理速度介于前两者之间，被广泛应用于中低档交换机中。

**参考答案**

（17）B

**试题（18）**

Cisco 路由器操作系统 IOS 有三种命令模式，其中不包括＿（18）＿。

（18）A．用户模式　　B．特权模式

C．远程连接模式　　D．置模式

**试题（18）分析**

Cisco 操作系统 IOS 有三种命令模式：

① router>

路由器处于用户模式，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器配置的内容。

② router#

在 router>提示符下键入 enable，路由器进入特权模式 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的配置内容。

③ router(config)#

在 router#提示符下键入 configure terminal，出现提示符 router(config)#，这时路由器处于全局配置状态，可以配置路由器的全局参数。如果输入某个端口标识，则可以进入局部配置状态。

```
router(config-if)#;
router(config-line)#;
router(config-router)#;…
```

这时可以配置路由器的局部参数。

**参考答案**

（18）C

**试题（19）**

通过 CATV 电缆访问因特网，在用户端必须安装的设备是＿（19）＿。

（19）A．ADSL Modem　　B．Cable Modem

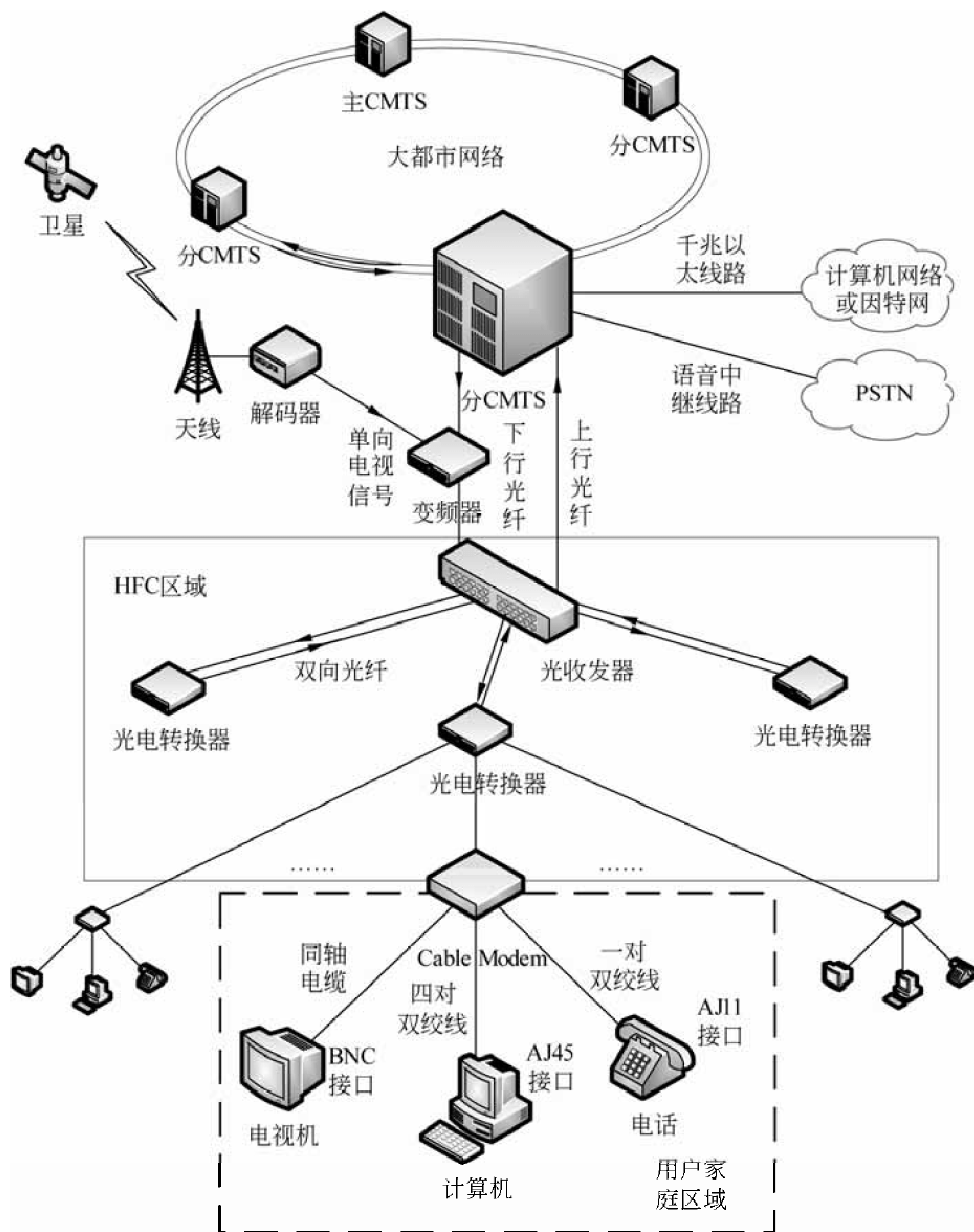
C．无线路由器　　D．以太网交换机

**试题（19）分析**

对传统的 CATV 网络进行改造就可以实现双向的数字传输业务，通过线缆调制解调器不需要拨号就能实现远程站点访问。可以采用一根上行、一根下行的双缆方式，也可以采用高频下行、低频上行的单缆方式。运营商通常采用混合光纤/铜缆（Hybrid Fiber/Coax，HFC）系统将 CATV 网络和运营商的高速光纤网络连接在一起。运营商一端的线缆调制解调器终接设备（CMTS）向大量的线缆调制解调器（Cable Modem，CM）提供高速连接。多数运营商借助于通用宽带路由器来实现 CMTS 功能，如下图所示。CMTS 的以太端口与以太网连接，同时通过中继线路连接 PSTN 网络，并将双向的计算机网络和语音信号调制，形成上行和下行的模拟信号，而单向的有线电视信号以频分复

用方式进入下行信号中。在 HFC 区域，借助于光收发器、光电转换器等设备完成信号的中继传输。

客户端与 CM 相连，并分解出有线电视、计算机网络和电话信号。典型的 CATV 系统提供 25～50Mb/s 的下行带宽和 2～3Mb/s 的上行带宽。




## 参考答案

（19）B

**试题（20）**

在互联网中可以采用不同的路由选择算法，所谓松散源路由是指 IP 分组__（20）__。

（20）A．必须经过源站指定的路由器

B．只能经过源站指定的路由器

C．必须经过目标站指定的路由器

D．只能经过目标站指定的路由器

**试题（20）分析**

在互联网中可以由源端指明到达目标的路由，这个功能是通过 IP 分组头中的选项实现的。所谓松散源路由是指传输的 IP 分组必须经过源端指定的路由器，但是也可能要经过源端没有指明的路由器；与此相反，所谓严格源路由则是指，传输的 IP 分组只能经过源端指定的路由器，而不能经过源端没有指定的路由器。

**参考答案**

（20）A

**试题（21）**

下面关于边界网关协议 BGP4 的描述中，不正确的是__（21）__。

（21）A．BGP4 网关向对等实体（Peer）发布可以到达的 AS 列表

B．BGP4 网关采用逐跳路由（hop-by-hop）模式发布路由信息

C．BGP4 可以通过路由汇聚功能形成超级网络（Supernet）

D．BGP4 报文直接封装在 IP 数据报中传送

**试题（21）分析**

现在通用的外部网关协议叫作 BGP（Border Gateway Protocol）。BGP 4 广泛地应用于不同 ISP 的网络（AS）之间，成为事实上的 Internet 外部路由协议标准。

BGP 4 是一种动态路由发现协议，支持无类别域间路由 CIDR。BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 的 4 种报文类型见下表，这些报文通过 TCP（179 端口）连接传送。

| 报 文 类 型 | 功 能 描 述 |
| --- | --- |
| 打开（Open） | 建立邻居关系 |
| 更新（Update） | 发送新的路由信息 |
| 保持活动状态（Keepalive） | 对 Open 的应答/周期性地确认邻居关系 |
| 通告（Notification） | 报告检测到的错误 |

**参考答案**

（21）D

**试题（22）**

RIP 协议中可以使用多种方法防止路由循环，在以下选项中不属于这些方法的

是__（22）__。

（22）A. 垂直翻转 B. 水平分割

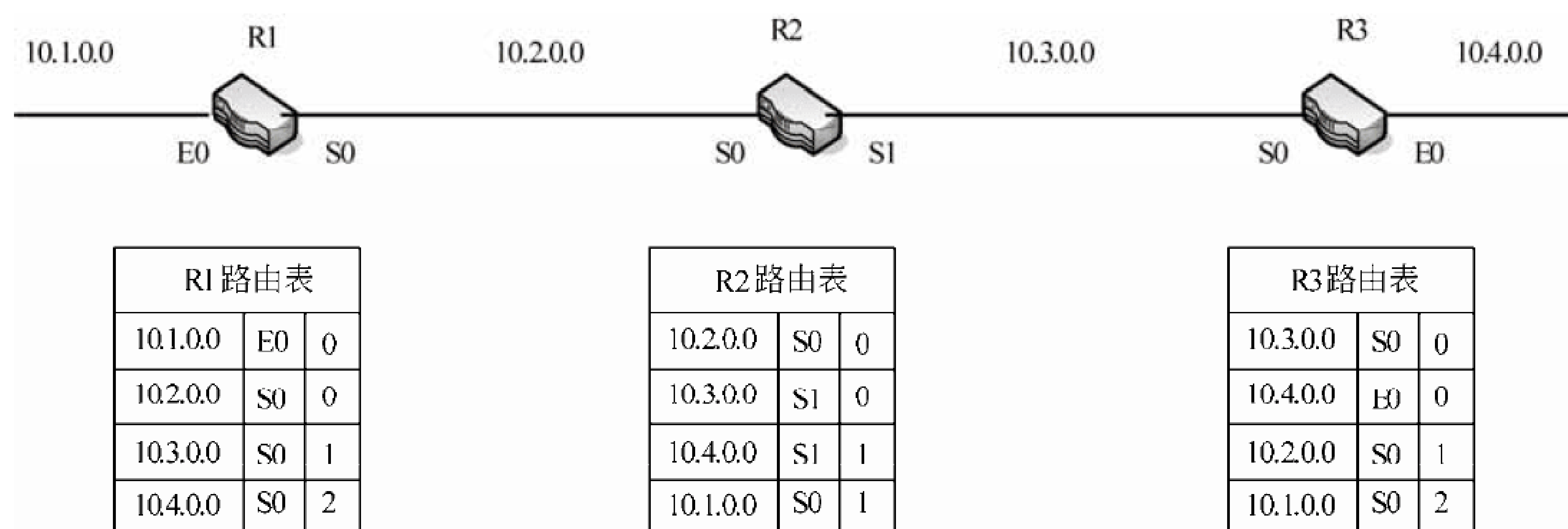
C. 反向路由毒化 D. 设置最大度量值

**试题（22）分析**

路由信息协议 RIP 采用距离矢量路由算法计算最佳路由。RIP 以跳步计数（hop count）作为路由费用的度量，允许的最大跳步数不超过 15 步。

距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。

例如在下图中，路由器 R1、R2、R3 的路由表已经收敛，每个路由表的后两项是通过交换路由信息而学习到的。如果在某一时刻，网络 10.4.0.0 发生故障，R3 检测到故障，并通过接口 S0 把故障通知 R2。如果 R2 在收到 R3 的故障通知前将其路由表发送到 R3，则 R3 会认为通过 R2 可以访问 10.4.0.0，并据此将路由表中第二条记录修改为（10.4.0.0，S0，2）。这样一来，路由器 R1、R2、R3 都认为通过其他的路由器存在一条通往 10.4.0.0 的路径，结果导致目标地址为 10.4.0.0 的数据包在三个路由器之间来回传递，从而形成路由环路，直至达到最大跳步数时才能终止循环传送过程。




| R1 路由表 | | |
|---|---|---|
| 10.1.0.0 | E0 | 0 |
| 10.2.0.0 | S0 | 0 |
| 10.3.0.0 | S0 | 1 |
| 10.4.0.0 | S0 | 2 |

| R2 路由表 | | |
|---|---|---|
| 10.2.0.0 | S0 | 0 |
| 10.3.0.0 | S1 | 0 |
| 10.4.0.0 | S1 | 1 |
| 10.1.0.0 | S0 | 1 |

| R3 路由表 | | |
|---|---|---|
| 10.3.0.0 | S0 | 0 |
| 10.4.0.0 | E0 | 0 |
| 10.2.0.0 | S0 | 1 |
| 10.1.0.0 | S0 | 2 |

解决路由环路问题可以采用水平分割法（Split Horizon）。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图 R2 的路由表项将加上一些注释，如下图所示，可以看出，每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。

简单的水平分割方案是"不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是"把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居"。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

| R2 路由表 | | | |
|---|---|---|---|
| 10.2.0.0 | S0 | 0 | 不发送给R1 |
| 10.3.0.0 | S1 | 0 | 不发送给R3 |
| 10.4.0.0 | S1 | 1 | 不发送给R3 |
| 10.1.0.0 | S0 | 1 | 不发送给R1 |

另外，前面提到的触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 R3 在接收 R2 的更新报文之前把网络 10.4.0.0 的故障告诉 R2，则也可以防止环路的形成。

**参考答案**

（22）A

**试题（23）**

RIP 协议默认的路由更新周期是＿（23）＿秒。

（23）A．30　　B．60　　C．90　　D．100

**试题（23）分析**

RIPv1（RFC 1058，1988）是早期的路由协议，使用本地广播地址 255.255.255.255 发布路由信息，默认的路由更新周期为 30 秒，持有时间（Hold-Down Time）为 180 秒。也就是说，RIP 路由器每 30 秒向所有邻居发送一次路由更新报文，如果在 180 秒之内没有从某个邻居接收到路由更新报文，则认为该邻居已经不存在了。这时如果从其他邻居收到了有关同一目标的路由更新报文，则用新的路由信息替换已失效的路由表项，否则，对应的路由表项被删除。

RIPv1 是有类别的协议（classful protocol），这意味着配置 RIPv1 时必须使用 A、B 或 C 类 IP 地址和子网掩码，例如不能把子网掩码 255.255.255.0 用于 B 类网络 172.16.0.0。

对于同一目标，RIP 路由表项中最多可以有 6 条等费用的通路，虽然默认是 4 条。RIP 可以实现等费用通路的负载均衡（equal-cost load balancing），这种机制提供了链路冗余功能，以对付可能出现的连接失效，但是 RIP 不支持不等费用通路的负载均衡，这种功能出现在后来的 IGRP 和 EIGRP 中。

RIPv2 是增强了 RIP 协议，定义在 RFC 1721 和 RFC 1722（1994）中。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是 RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制路由更新信息的传播。其他方面的特性

与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

**参考答案**

（23）A

**试题（24）、（25）**

OSPF 协议适用于 4 种网络。下面的选项中，属于广播多址网络的是<u>（24）</u>，属于非广播多址网络的是<u>（25）</u>。

（24）A. Ethernet　B. PPP　C. Frame Relay　D. RARP

（25）A. Ethernet　B. PPP　C. Frame Relay　D. RARP

**试题（24）、（25）分析**

OSPF（RFC 2328，1998）是一种链路状态协议，用于在自治内部的路由器之间交换路由信息。OSPF 具有支持大型网络、占用网络资源少、路由收敛快等优点，在目前的网络配置中占有重要的地位。

距离矢量协议发布自己的路由表，交换的路由信息量很大。链路状态协议与之不同，它是从各个路由器收集链路状态信息，构造网络拓扑结构图，使用 Dijkstra 的最短通路优先算法（Shortest Path First，SPF）计算到达各个目标的最佳路由。

网络的物理连接和拓扑结构不同，交换路由信息的方式就不同。OSPF 将路由器连接的物理网络划分为 4 种类型：

① 点对点网络：例如一对路由器用 64Kb 的串行线路连接，就属于点对点网络，在这种网络中，两个路由器可以直接交换路由信息。

② 广播多址网络：以太网（Ethernet）或者其他具有共享介质的局域网都属于这种网络。在这种网络中，一条路由信息可以广播给所有的路由器。

③ 非广播多址网络（non-broadcast multi-access，NBMA）：例如 X.25 分组交换网或帧中继网络就属于这种网络，在这种网络中可以通过组播方式发布路由信息。

④ 点到多点网络：可以把非广播网络当作多条点对点网络来使用，从而把一条路由信息发送到不同的目标，RARP 协议就是以这种方式工作的。

**参考答案**

（24）A　（25）C

**试题（26）**

MPLS（多协议标记交换）根据标记对分组进行交换，MPLS 包头的位置应插入在<u>（26）</u>。

（26）A. 以太帧头的前面　B. 以太帧头与 IP 头之间

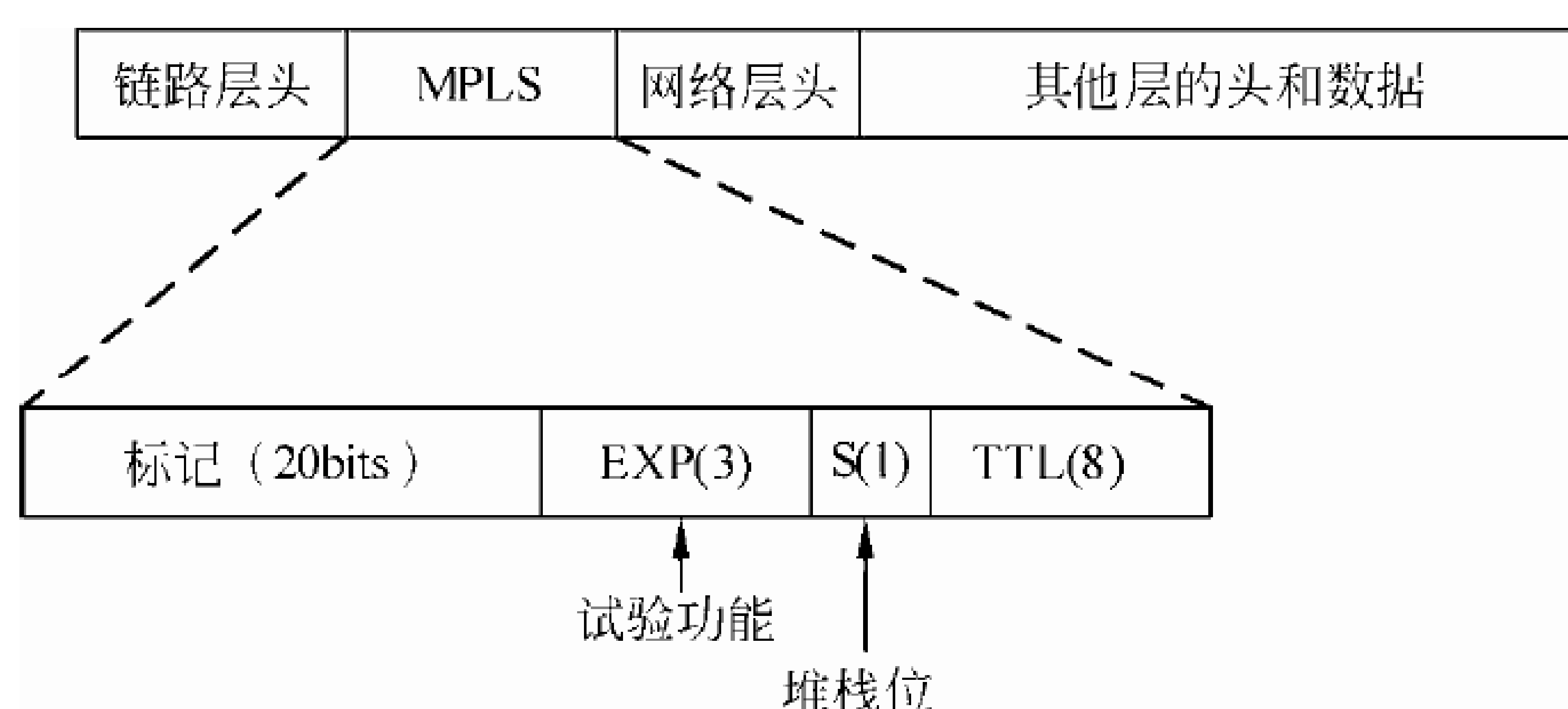
C. IP 头与 TCP 头之间　D. 应用数据与 TCP 头之间

**试题（26）分析**

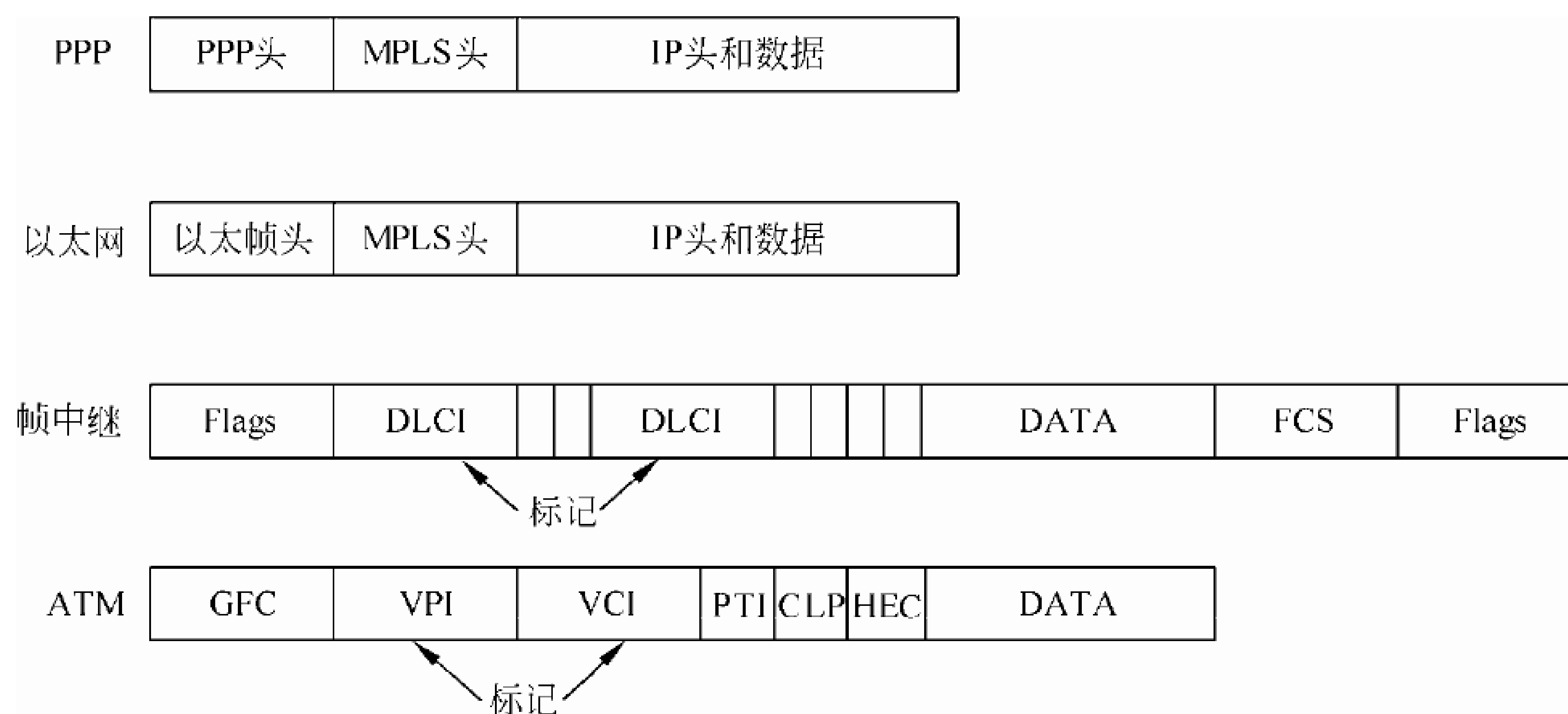
所谓第三层交换是指利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换与路由不同，前者用硬件实现，速度快，而后者由软件实现，速度慢。

三层交换机的工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住目标 MAC 地址和源 MAC 地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧时就直接进行交换了，不再调用路由功能。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

IETF 开发的多协议标记交换（Multi-protocol Label Switching，MPLS，RFC3031）把第 2 层的链路状态信息（带宽、延迟、利用率等）集成到第 3 层的协议数据单元中，从而简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层，标准格式如下图所示。




MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包，甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等，如下图所示。




**参考答案**

（26）B

**试题（27）**

IGRP 协议的路由度量包括多种因素，但是在一般情况下可以简化为＿（27）＿。

（27）A．可靠性 B．带宽 C．跳步数 D． MTU

**试题（27）分析**

IGRP是Cisco公司开发的路由协议。它也是一个距离矢量协议，但是与RIP相比，它有下列优点：

① 使用了带宽和延迟等参数作为路由度量标准；
② 利用触发更新来加快路由收敛；
③ 支持不等费用通路的负载均衡；
④ 最大跳步数扩充到255，可以支持更大的网络。

IGRP不使用跳步数作为路由度量，虽然在一般情况下可以简化为跳步数。IGRP的路由度量因素包括带宽、延迟、可靠性、负载和MTU，其中前两者是默认的，但是可以通过配置加入其他参数。可靠性和负载划分为1～255级，可靠性1是最低的，可靠性255是最高的，负载1使用最少，负载255是百分之百利用的。MTU指最大帧长度，在实际运行中，它是一个常数值，通常采用一条通路中最小的MTU值。这些因素综合起来作为路由费用的度量，使得IGRP可以选择更好的路由。相对于RIP的跳步计数，IGRP协议的路由选择更加合理。

IGRP的路由更新周期是90秒，持有时间是280秒，为了加速收敛，采用了触发更新技术。

**参考答案**

（27）C

**试题（28）**

采用Windows Server 2003创建一个Web站点，主目录中添加主页文件index.asp后，在客户机的浏览器地址栏内输入该网站的域名后不能正常访问，则不可能的原因是__（28）__。

（28）A．Web站点配置完成后没有重新启动
B．DNS服务器不能进行正确的域名解析
C．没有将index.asp添加到该Web站点的默认启动文档中
D．没有指定该Web站点的服务端口

**试题（28）分析**

本题考查Windows Server 2003 Web服务器的配置。

采用Windows Server 2003创建一个Web站点时，通常是先安装IIS建立网站，然后对网站进行配置，重新启动系统生效。若Web站点配置完成后没有重新启动，或DNS服务器不能进行正确的域名解析，以及没有将index.asp添加到该Web站点的默认启动文档中都可能导致站点无法正常访问。若没有配置站点的服务端口系统会默认为80，故正确答案为D。

**参考答案**

（28）D

**试题（29）**

DNS 服务器在名称解析过程中正确的查询顺序为__（29）__。

（29）A．本地缓存记录→区域记录→转发域名服务器→根域名服务器
B．区域记录→本地缓存记录→转发域名服务器→根域名服务器
C．本地缓存记录→区域记录→根域名服务器→转发域名服务器
D．区域记录→本地缓存记录→根域名服务器→转发域名服务器

**试题（29）分析**

DNS 服务器在名称解析过程中，首先查询本地缓存，若缓存中没有被查域名的记录，则在本区域主域名服务器中进行查找，紧接着查询转发域名服务器，最后是根域名服务器，因此，正确的查询顺序为：本地缓存记录→区域记录→转发域名服务器→根域名服务器。

**参考答案**

（29）A

**试题（30）**

DNS 服务器进行域名解析时，若采用递归方法，发送的域名请求为__（30）__。

（30）A．1 条　B．2 条　C．3 条　D．多条

**试题（30）分析**

DNS 服务器进行域名解析时，若采用递归方法，发出 1 条请求后，类似于程序递归的思想，最终只有一条结果返回。若采用迭代方法，每次返回的是上一级查到的可提供解析的地址，因此会有多条域名请求发出。

**参考答案**

（30）A

**试题（31）**

若 DNS 资源记录中记录类型（record-type）为 A，则记录的值为__（31）__。

（31）A．名字服务器　B．主机描述　C．IP 地址　D．别名

**试题（31）分析**

DNS 服务器中主要的资源记录有 A（域名到 IP 地址的映射）、PTR（IP 地址到域名的映射）、MX（邮件服务器及其优先级）、CNAM（别名）和 NS（区域的授权服务器）等类型。通过 A 记录可以由域名查地址，也可以由地址查域名。

**参考答案**

（31）C

**试题（32）、（33）**

FTP 客户上传文件时，通过服务器 20 端口建立的连接是__（32）__，客户端应用进程的端口可以为__（33）__。

（32）A．建立在 TCP 之上的控制连接　B．建立在 TCP 之上的数据连接
C．建立在 UDP 之上的控制连接　D．建立在 UDP 之上的数据连接

（33）A．20　　B．21　　C．80　　D．4155

**试题（32）、（33）分析**

FTP 客户机与服务器之间建立两条 TCP 连接，一条用于传送控制信息（端口号为21），另一条用于传送文件内容（端口号为 20）。客户端应用进程的端口应该为高端（端口号大于 1024）。

**参考答案**

（32）B　（33）D

**试题（34）**

在 Linux 系统中，命令__（34）__用于管理各项软件包。

（34）A.install　　B．rpm　　C.fsck　　D．msi

**试题（34）分析**

本题考查 linux 系统下 rpm 命令的基本概念。

RPM 全称为 Redhat Package Manager，它是许多流行的 Linux 发行版的软件包管理工具。

**参考答案**

（34）B

**试题（35）**

Linux 系统中，为某一个文件在另外一个位置建立一个文件链接的命令为__（35）__。

（35）A.ln　　B．copy　　C．locate　　D．cat

**试题（35）分析**

本题考查 Linux 系统下文件操作命令 ln 的基本概念。

ln 命令在两个文件之间创建链接。

**参考答案**

（35）A

**试题（36）**

默认情况下，Linux 系统中用户登录密码信息存放在__（36）__文件中。

（36）A．/etc/group　　B．/etc/userinfo

C．/etc/shadow　　D．/etc/profie

**试题（36）分析**

本题考查 Linux 系统下 shadow 文件的基本概念。

Shadow 文件用于存储 Linux 系统中用户账号密码配置文件。

**参考答案**

（36）C

**试题（37）**

若要显示 IP 路由表的内容，可以使用命令__（37）__。

（37）A．Netstat-s　　B．Netstat-r　　C．Netstat-n　　D．Netstat-a

**试题（37）分析**

本题考查常用网络命令。

Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的信息，其中参数 r 用于打印当前系统的路由信息。

**参考答案**

（37）B

**试题（38）**

下列命令中，不能查看网关 IP 地址的是＿（38）＿。

（38）A．Nslookup　B．Tracert　C．Netstat　D．Route print

**试题（38）分析**

本题考查常用网络命令。

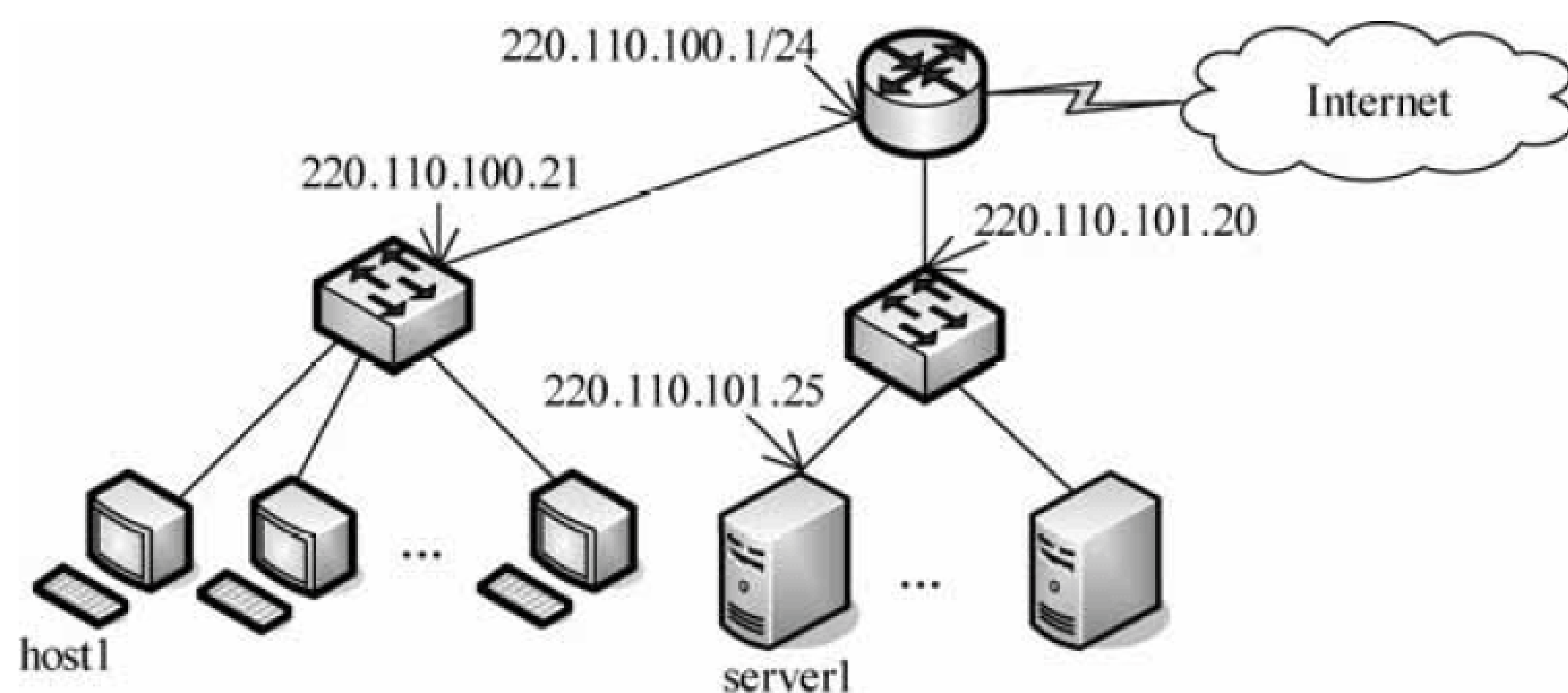
Tracert、Netstat 及 Route print 均可以获得网关 IP 地址信息。

**参考答案**

（38）A

**试题（39）、（40）**

某网络拓扑如下图所示，在主机 host1 上设置默认路由的命令为＿（39）＿；在主机 host1 上增加一条到服务器 server1 主机路由的命令为＿（40）＿。




（39）A．route add 0.0.0.0 mask 0.0.0.0 220.110.100.1

B．route add 220.110.100.1 0.0.0.0 mask 0.0.0.0

C．add route 0.0.0.0 mask 0.0.0.0 220.110.100.1

D．add route 220.110.100.1 0.0.0.0 mask 0.0.0.0

（40）A．add route 220.110.100.1 220.110.101.25. mask 255.255.255.0

B．route add 220.110.101.25. mask 255.255.255.0 220.110.100.1

C．route add 220.110.101.25. mask 255.255.255.255 220.110.100.1

D．add route 220.110.100.1 220.110.101.25. mask 255.255.255.255

**试题（39）、（40）分析**

Route 命令的功能是显示和修改本地的 IP 路由表，其语法如下：

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]]
[if Interface]]
```

例如，若要对网关地址 220.110.100.1 要添加一条默认路由，则命令为：

```
route add 0.0.0.0 mask 0.0.0.0 220.110.100.1
```

在主机 host1 上增加一条到服务器 server1 主机路由，需要指定 server1 的 IP 地址，掩码为 255.255.255.255，下一跳为 host1 所在网络的网关，即 route add 220.110.101.25. mask 255.255.255.255 220.110.100.1。

**参考答案**

（39）A　（40）C

**试题（41）**

在 SNMPv3 中，把管理站（Manager）和代理（Agent）统一叫作___（41）___。

（41）A．SNMP 实体　　B．SNMP 引擎
　　C．命令响应器　　D．命令生成器

**试题（41）分析**

本题考查 SNMP 协议的基础知识。

按照 SNMP 协议的体系结构，网络管理系统由管理站（Manager）和代理（Agent）两种功能实体组成。

在 SNMPv3 中管理站（Manager）和代理（Agent）两种功能实体统一叫作 SNMP 实体（SNMP entity）。实体是体系结构的一种实现，由一个或多个 SNMP 引擎（SNMP engine）和一个或者多个 SNMP 应用（SNMP Application）组成。

SNMPv3 的应用程序分为命令生成器、命令响应器、通知发送器、通知接收器和代理转发器 5 种。

**参考答案**

（41）A

**试题（42）**

下列选项中，同属于报文摘要算法的是___（42）___。

（42）A．DES 和 MD5　　B．MD5 和 SHA-1
　　C．RSA 和 SHA-1　　D．DES 和 RSA

**试题（42）分析**

本题考查安全算法相关常识。

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，从而使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。

常见加密算法有：DES（Data Encryption Standard）、3DES（Triple DES）、RC2 和 RC4、IDEA（International Data Encryption Algorithm）、RSA。

报文摘要算法主要应用在“数字签名”领域，作为对明文的摘要算法。著名的摘要

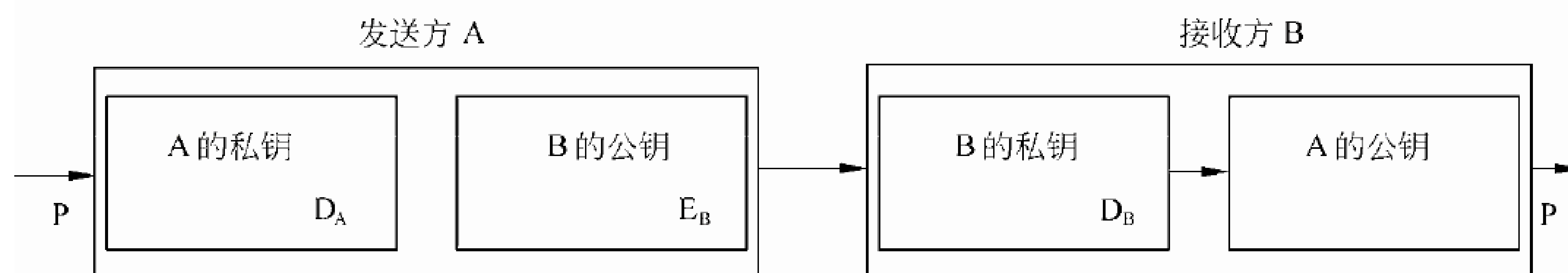
算法有 RSA 公司的 MD5 算法和 SHA1 算法及其大量的变体。

**参考答案**

（42）B

**试题（43）、（44）**

下图所示为一种数字签名方案，网上传送的报文是__（43）__，防止 A 抵赖的证据是__（44）__。




（43）A．P　　B．$D_A(P)$　　C．$E_B(D_A(P))$　　D．$D_A$

（44）A．P　　B．$D_A(P)$　　C．$E_B(D_A(P))$　　D．$D_A$

**试题（43）、（44）分析**

本题考查数字签名的实现过程。

题图中所示为一种利用公钥加密算法实现的数字签名方案，发送方 A 要发送给接收方 B 的报文 P 经过 A 的私钥签名和 B 的公钥加密后形成报文 $E_B(D_A(P))$发送给 B，B 利用自己的私钥 $D_B$ 和 A 的公钥 $E_A$ 对消息 $E_B(D_A(P))$进行解密和认证后得到报文 P，并且保存经过 A 签名的消息 $D_A(P)$作为防止 A 抵赖的证据。

**参考答案**

（43）C　（44）B

**试题（45）**

下面关于域本地组的说法中，正确的是__（45）__。

（45）A．成员可来自森林中的任何域，仅可访问本地域内的资源

B．成员可来自森林中的任何域，可访问任何域中的资源

C．成员仅可来自本地域，仅可访问本地域内的资源

D．成员仅可来自本地域，可访问任何域中的资源

**试题（45）分析**

本题考查 Windows Server 2003 活动目录中用户组的概念。

在 Windows Server 2003 的活动目录中，用户分为全局组（Global Groups）、域本地组（Domain Local Groups）和通用组（Universal Groups）。其中全局组成员来自于同一域的用户账户和全局组，可以访问域林中的任何资源；域本地组成员来自森林中任何域中的用户账户、全局组和通用组以及本域中的域本地组，只能访问本地域中的资源；通用组成员来自森林中任何域中的用户账户、全局组和其他的通用组，可以授予多个域中

的访问权限。

**参考答案**

（45）A

**试题（46）、（47）**

在 Kerberos 认证系统中，用户首先向___（46）___申请初始票据，然后从___（47）___获得会话密钥。

（46）A．域名服务器 DNS　　B．认证服务器 AS
　　C．票据授予服务器 TGS　　D．认证中心 CA

（47）A．域名服务器 DNS　　B．认证服务器 AS
　　C．票据授予服务器 TGS　　D．认证中心 CA

**试题（46）、（47）分析**

本题考查 Kerberos 认证系统的基础知识。

Kerberos 认证系统的认证过程如下图所示。

① 用户向认证服务器 AS 申请初始票据；

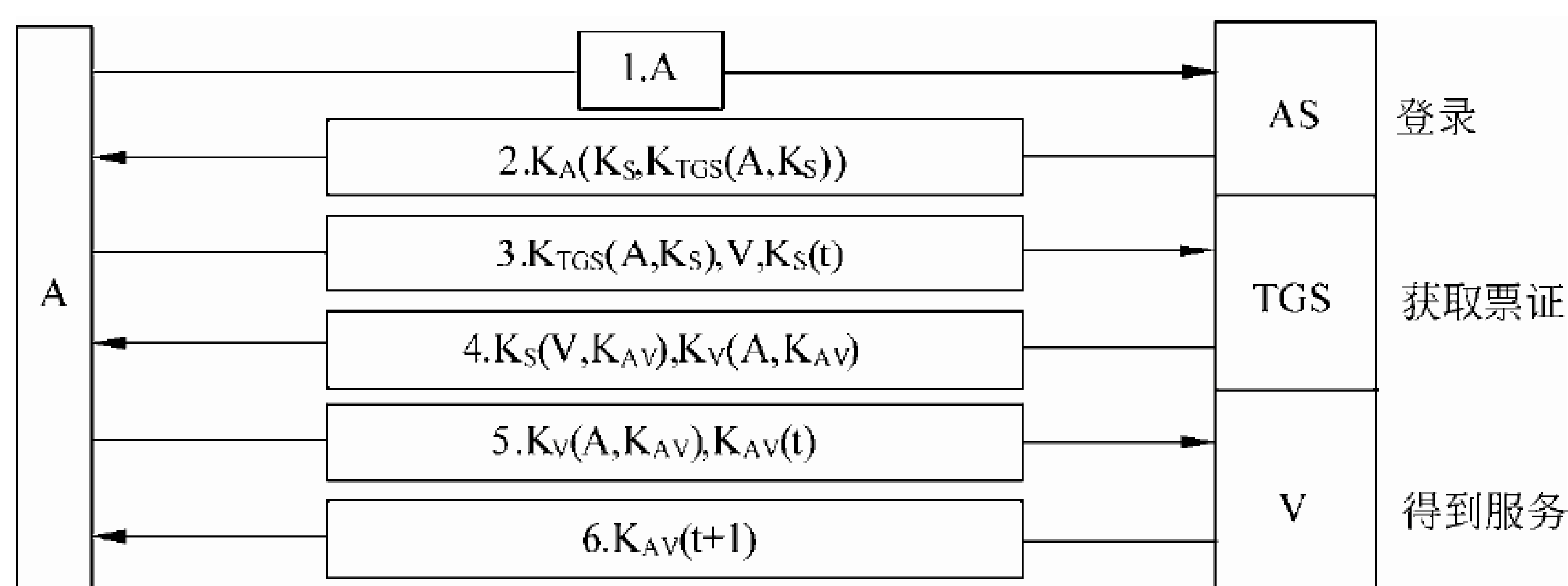
② 认证服务器 AS 向用户发放票据授予票据（TGT）；

③ 用户向 TGS 请求会话票据；

④ TGS 验证用户身份后发放给用户会话票据 $K_{AV}$；

⑤ 用户向应用服务器请求登录；

⑥ 应用服务器向用户验证时间戳。




**参考答案**

（46）B　（47）C

**试题（48）、（49）**

HTTPS 的安全机制工作在___（48）___，而 S-HTTP 的安全机制工作在___（49）___。

（48）A．网络层　　B．传输层　　C．应用层　　D．物理层

（49）A．网络层　　B．传输层　　C．应用层　　D．物理层

**试题（48）、（49）分析**

本题考查安全协议的概念。

安全的超文本传输协议（Secure HTTP，S-HTTP）是一个面向报文的安全通信协议，是 HTTP 协议的扩展，位于应用层。

SSL/TLS 位于传输层，SSL/TLS 在 Web 安全通信中被称为 HTTPS。

**参考答案**

（48）B　（49）C

**试题（50）**

下面病毒中，属于蠕虫病毒的是__（50）__。

（50）A．Worm.Sasser 病毒　　B．Trojan.QQPSW 病毒

C．Backdoor.IRCBot 病毒　　D．Macro.Melissa 病毒

**试题（50）分析**

本题考查计算机病毒的基础知识。

病毒文件名称一般分为三部分，第一部分表示病毒的类型，如 Worm 表示蠕虫病毒，Trojan 表示特洛伊木马，Backdoor 表示后门病毒，Macro 表示宏病毒等。

**参考答案**

（50）A

**试题（51）**

互联网规定的 B 类私网 IP 地址为__（51）__。

（51）A．172.16.0.0/16　　B．172.16.0.0/12

C．172.15.0.0/16　　D．172.15.0.0/12

**试题（51）分析**

私网地址不能在公网上出现，只能用在内部网络中，所有的路由器都不转发目标地址为私网地址的数据报。下面的地址都是私网地址：

- 10.0.0.0～10.255.255.255　　1 个 A 类地址
- 172.16.0.0～172.31.255.255　　16 个 B 类地址
- 192.168.0.0～192.168.255.255　　256 个 C 类地址

**参考答案**

（51）B

**试题（52）、（53）**

如果一个公司有 2000 台主机，则必须给它分配__（52）__个 C 类网络。为了使该公司网络在路由表中只占一行，指定给它的子网掩码应该是__（53）__。

（52）A．2　　B．8　　C．16　　D．24

（53）A．255.192.0.0　　B．255.240.0.0　　C．255.255.240.0　　D．255.255.248.0

**试题（52）、（53）分析**

无类别的域间路由（Classless Inter-Domain Routing，CIDR）技术解决路由缩放问题。所谓路由缩放有两层含义：其一是对于大多数中等规模的组织没有适合的地址空间，这样的组织一般拥有几千台主机，C 类网络太小，只有 254 个地址，B 类网络太大，有 65 000 多个地址，A 类网络就更不用说了，况且 A 类和 B 类地址也快分配完了；其二是路由表增长太快，如果所有的 C 类网络号都在路由表中占一行，这样的路由表就太大了，其查找速度无法达到满意的程度。CIDR 技术就是解决这两个问题的，它可以把若干个 C 类网络分配给一个用户，并且在路由表中只占一行，这是一种将大块的地址空间合并为少量路由信息的策略。

由于一个 C 类网络可以提供 254 个主机地址，所以 2000 个地址需要 8 个 C 类网络。把 8 个 C 类网络汇聚成一个超网地址，使用的网络掩码为 255.255.248.0。

**参考答案**

（52）B （53）D

**试题（54）**

ISP 分配给某公司的地址块为 199.34.76.64/28，则该公司得到的地址数是__（54）__。

（54）A．8 B．16 C．32 D．64

**试题（54）分析**

地址块 199.34.76.64/28 的二进制形式如下：

11000111.00100010.01001100.01000000

11111111.1111 1111.1111 1111.11110000

由于网络掩码占用了 28 位，只有 4 位留给主机地址，所以只有 16 个地址（包括全 0 和全 1 地址）。

**参考答案**

（54）B

**试题（55）**

由 16 个 C 类网络组成一个超网（supernet），其网络掩码（mask）应为__（55）__。

（55）A．255.255.240.16 B．255.255.16.0

C．255.255.248.0 D．255.255.240.0

**试题（55）分析**

16 个 C 类网络组成一个超网，其网络掩码（mask）应为 255.255.240.0。

**参考答案**

（55）D

**试题（56）**

设 IP 地址为 18.250.31.14，子网掩码为 255.240.0.0，则子网地址是__（56）__。

（56）A．18.0.0.14 B．18.31.0.14

C．18.240.0.0　　D．18.9.0.14

**试题（56）分析**

IP 地址 18.250.31.14/255.240.0.0 的二进制形式为：

00010010.11111010.00011111.00001110

11111111. 11110000.00000000.00000000

则子网地址是 00010010.11110000.00000000.00000000，即 18.240.0.0。

**参考答案**

（56）C

**试题（57）**

IPv6 的“链路本地地址”是将主机的__（57）__附加在地址前缀 1111 1110 10 之后产生的。

（57）A．IPv4 地址　　B．MAC 地址

C．主机名　　D．任意字符串

**试题（57）分析**

IPv6 中的链路本地地址是将主机网卡的 MAC 地址附加在链路本地地址前缀 1111 1110 10 之后形成的。链路本地地址用于同一链路相连的结点间通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址（APIPA），可用于邻居发现，并且总是自动配置的，包含链路本地地址的分组不会被路由器转发。

**参考答案**

（57）B

**试题（58）**

如果要设置交换机的 IP 地址，则命令行提示符应该是__（58）__。

（58）A．Switch >　　B．Switch#

C．Switch(config) #　　D．Switch (config-if)#

**试题（58）分析**

如果要设置交换机的 IP 地址，应进入全局配置模式，其命令行提示符为 Switch (config) #，Switch(config-if) #为端口配置模式，Switch#为特权模式，Switch >为用户模式。

**参考答案**

（58）C

**试题（59）**

路由器命令“Router(config-subif)# encapsulation dot1q 1”的作用是__（59）__。

（59）A．设置封装类型和子接口连接的 VLAN 号

B．进入 VLAN 配置模式

C．配置 VTP 口号

D．指定路由器的工作模式

**试题（59）分析**

路由器命令“Router(config-subif)# encapsulation dot1q 1”的作用是设置封装类型为 802.1q，子接口连接的虚拟局域网编号为 VLAN 1。

**参考答案**

（59）A

**试题（60）**

若路由器显示的路由信息如下，则最后一行路由信息是怎样得到的？__（60）__。

R3#show ip route

Gateway of last resort is not set

192.168.0.0/24 is subnetted, 6 subnets

C 192.168.1.0 is directly connected, Ethernet0

C 192.168.65.0 is directly connected, Serial0

C 192.168.67.0 is directly connected, Serial1

R 192.168.69.0 [120/1] via 192.168.67.2, 00:00:15, Serial1

[120/1] via 192.168.65.2, 00:00:24, Serial0

R 192.168.5.0 [120/1] via 192.168.67.2, 00:00:15, Serial1

R 192.168.3.0 [120/1] via 192.168.65.2, 00:00:24, Serial0

（60）A．串行口直接连接的　　　　B．由路由协议发现的

C．操作员手工配置的　　　　D．以太网端口直连的

**试题（60）分析**

对路由表中的最后一项 R 192.168.3.0 [120/1] via 192.168.65.2, 00:00:24, Serial0 解释如下：

① R——表示该路由是由 RIP 协议获取的，C 代表直接相连的网段；

② 192.168.3.0——表示目标网段；

③［120/1］——120 表示 RIP 的管理距离（默认值），1 是该路由的度量值（跳数）；

④ Via——经由的意思；

⑤ 192.168.65.2——表示从当前路由器出发到达目标的下一跳点的 IP 地址；

⑥ 00:00:24——表示该条路由产生的时间；

⑦ Serial0——表示该路由的输出端口。

**参考答案**

（60）B

**试题（61）**

按照 802.1d 生成树协议（STP），在交换机互连的局域网中，__（61）__的交换机被选为根交换机。

（61）A．MAC 地址最小的　　　　B．MAC 地址最大的

C．ID 最小的　　D．ID 最大的

**试题（61）分析**

按照 802.1d 生成树协议（STP），在交换机互连的局域网中，ID 最小的交换机被选为根交换机。网桥或交换机 ID 由优先级和 MAC 地址两部分组成。

**参考答案**

（61）C

**试题（62）**

以太网中采用了二进制指数后退算法，这个算法的特点是 __(62)__ 。

（62）A．网络负载越轻，可能后退的时间越长

B．网络负载越重，可能后退的时间越长

C．使得网络既可以适用于突发性业务，也可以适用于流式业务

D．可以动态地提高网站发送的优先级

**试题（62）分析**

在检测到冲突时，为减少再一次冲突的概率，按照下面的二进制指数后退算法计算后退时间：随着重发次数 $n$ 的增加，后退时延 $t_\xi$的取值按 2 的指数增大。即：第一次试发送时 $n$ 值为 0，每冲突一次 $n$ 的值加 1，并按下式计算后退时延

$$\begin{cases} \xi = \mathrm{random}[0, 2^n] \\ t_\xi = \xi\tau \end{cases}$$

其中，$\tau$（网络最大传播时延的 2 倍）是一个很重要的参数，表示网络上检测冲突的最长时间。上面第一式表示在区间$[0，2^n]$中取一均匀分布的随机整数$\xi$，第二式的作用是计算出随机后退时延。按照这种方法，网络负载越重，可能后退的时间越长。

为了避免无限制的重发，要对重发次数 $n$ 进行限制，当 $n$ 增加到某一最大值（例如 16）时停止发送，并向上层协议报告发现的错误。

**参考答案**

（62）B

**试题（63）**

以太网帧格式如下图所示，其中“填充”字段的作用是 __(63)__ 。

| 前导字段 | 帧起始符 | 目的地址 | 源地址 | 长度 | 数据 | 填充 | 校验和 |
|---|---|---|---|---|---|---|---|

（63）A．可用于表示任选参数　　B．表示封装的上层协议

C．表示控制帧的类型　　D．维持 64 字节的最小帧长

**试题（63）分析**

以太网规定了最小帧长，以避免在发送的过程中检测不到冲突。如果帧中包含的数据较少，则要填充冗余字节，以便补充到 64 字节的最小帧长。

**参考答案**

（63）D

**试题（64）**

IEEE 802.11 采用了 CSMA/CA 协议，下面关于这个协议的描述中错误的是（64）。

（64）A. 各个发送站在两次帧间隔（IFS）之间进行竞争发送

B. 每一个发送站维持一个后退计数器并监听网络上的通信

C. 各个发送站按业务的优先级获得不同的发送机会

D. CSMA/CA 协议适用于突发性业务

**试题（64）分析**

CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫作载波监听多路访问/冲突避免协议。在无线网中进行冲突检测是有困难的。例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔（Inter Frame Spacing，IFS）时间。另外还有一个后退计数器，它的初始值是由随机数发生器设置的，递减计数直到 0。基本的操作过程是：

① 如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

② 听到信道空闲后等待一个 IFS 时间，然后开始计数。最先计数完的站开始发送。

③ 其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成后开始发送。

分析这个算法发现，两次 IFS 之间的间隔是各个站竞争发送到时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

**参考答案**

（64）C

**试题（65）**

在 IEEE 802.11 标准中使用了扩频通信技术，下面选项中有关扩频通信的说法中正确的是（65）。

（65）A. 扩频技术是一种带宽很宽的红外线通信技术

B. 扩频技术就是用伪随机序列对代表数据的模拟信号进行调制

C. 扩频通信系统的带宽随着数据速率的提高而不断扩大

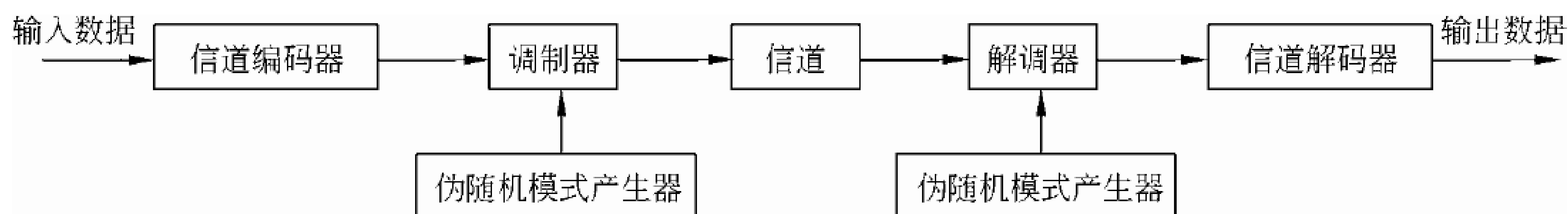
D. 扩频技术扩大了频率许可证的使用范围

**试题（65）分析**

IEEE 802.11WLAN 中使用扩展频谱通信技术，这种技术的特点是将信号散布到更宽的频带上以减少发生阻塞和干扰的机会。有两种扩频方式，一种是频率跳动扩频（Frequency Hopping Spread Spectrum，FHSS），另外一种是直接序列扩频（Direct Sequence

Spread Spectrum，DSSS）。

下图表示各种扩展频谱系统的共同特点。输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号。再用一个伪随机序列对这个信号进行调制。调制的结果是大大拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后再进入信道解码器来恢复数据。




伪随机序列由一个使用初值（称为种子）的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计的好，得到的序列还是能够通过各种随机性测试的，这就是被叫作伪随机序列的原因。除非你知道算法与种子，否则预测序列是不可能的。因此只有与发送器共享一个伪随机序列的接收器才能对信号进行解码。

**参考答案**

（65）B

**试题（66）**

Wi-Fi联盟制定的安全认证方案WPA（Wi-Fi Protected Access）是＿（66）＿标准的子集。

（66）A．IEEE 802.11　　B．IEEE 802.11a
C．IEEE 802.11b　　D．IEEE 802.11i

**试题（66）分析**

Wi-Fi（Wireless Fidelity）是无线通信技术的商标，由 Wi-Fi 联盟（Wi-Fi Alliance）所持有，使用在经过认证的IEEE 802.11产品上，其目的是改善基于 IEEE 802.11 标准的网络产品之间的兼容性。

无线网络中的安全问题从暴露到最终解决经历了相当长的时间。这期间，Wi-Fi联盟的厂商们迫不及待地以 802.11i 草案的一个子集为蓝图制定了称为WPA（Wi-Fi Protected Access）的安全认证方案，以便在市场上及时推出新的无线网络产品。

在 WPA 的设计中包含了认证、加密和数据完整性校验三个组成部分。首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以 128 比特的密钥和 48 位的初始向量（IV）用于RC4加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议（Temporary Key Integrity Protocol，TKIP），以更频繁地变换密钥来减少安全风险。最后，WPA 强化了数据完整性保护。在IEEE 802.11 标准中定义的 WEP 协议使用的循环冗余校验方法具有先天性缺陷，在不知道 WEP 密钥的情况下，要篡改分组和对应的 CRC 也是可能的。WPA 使用报文完整性编码来检测伪

造的数据包，并且在报文认证码中包含有帧计数器，还可以防止重放攻击。

IEEE 802.11i 标准正式发布后，Wi-Fi 联盟就按照新的安全标准对无线产品进行认证，并且把这种认证方案称为 WPA2。

**参考答案**

（66）D

**试题（67）**

为了确定一个网络是否可以连通，主机应该发送 ICMP （67） 报文。

（67）A．回声请求　　B．路由重定向
　　　C．时间戳请求　　D．地址掩码请求

**试题（67）分析**

ICMP（Internet control Message Protocol）与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠的提交。ICMP 报文的格式如下所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

| 类　型 | 代 码 | 校验和 |
|---|---|---|
| 参　数 | | |
| 信息（可变长） | | |

下面解释 ICMP 各类报文的含义。

① 目标不可到达（类型 3）：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。

② 超时（类型 11）：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。

③ 源抑制（类型 4）：这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。

④ 参数问题（类型 12）：如果路由器或主机判断出 IP 头中的字段或语义出错，则

返回这种报文，报文头中包含一个指向出错字段的指针。

⑤ 路由重定向（类型 5）：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。

⑥ 回声（请求/响应，类型 8/0）：用于测试两个结点之间的通信线路是否畅通。收到回声请求的结点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。

⑦ 时间戳（请求/响应，类型 13/14）：用于测试两个结点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

⑧ 地址掩码（请求/响应，类型 17/18）：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标结点与源结点是否在同一 LAN 中。

**参考答案**

（67）A

**试题（68）**

在域名系统中，根域下面是顶级域（TLD）。在下面的选项中 __（68）__ 属于全世界通用的顶级域。

（68）A. org　　B. cn　　C. microsoft　　D. mil

**试题（68）分析**

域名系统 DNS 的逻辑结构是一个分层的域名树，Internet 网络信息中心（Internet Network Information Center，InterNIC）管理着域名树的根，称为根域。根域没有名称，用圆点“.”表示，是域名空间的最高级别。在 DNS 的名称中，有时在末尾附加一个“.”，就是表示根域，但经常是省略的。DNS服务器可以自动补上结尾的圆点，也可以处理结尾带圆点的域名。

根域下面是顶级域（Top-Level Domains，TLD），分为国家顶级域（country code Top Level Domain，ccTLD）和通用顶级域（generic Top Level Domain，gTLD）。国家顶级域名包含 243 个国家和地区代码，例如 cn 代表中国，uk 代表英国等。最初的通用顶级域有 7 个，如下表所示，这些顶级域名原来主要供美国使用，随着 Internet 的发展，com、org 和 net 成为全世界通用的顶级域名，这就是所谓的国际域名，而 edu、gov 和 mil 则限于美国使用。

| com | 商业机构等盈利性组织 |
|---|---|
| edu | 教育机构，学术组织，国家科研中心等 |
| gov | 美国非军事性的政府机关 |
| mil | 美国的军事组织 |
| net | 网络信息中心（NIC）和网络操作中心（BIC）等 |
| org | 非盈利性组织，例如技术支持小组，计算机用户小组等 |
| int | 国际组织 |

负责互联网域名注册的服务商ICANN在2000年11月决定，从2001年开始使用7个新的国际顶级域名：biz（商业机构）、info（网络公司）、name（个人网站）、pro（医生和律师等职业人员）、aero（航空运输业专用）、coop（商业合作社专用）和museum（博物馆专用），其中前4个是非限制性域名，后3个限于专门的行业使用，受有关行业组织的管理。

2008年6月，ICANN在巴黎年会上通过了个性化域名方案，可以用公司名字为结尾的域名，例如ibm、hp、qq等。可以认为，这些域名的所有者在某种意义上就是一个域名注册机构，今后将会有无穷多的国际域名。

顶级域下面是二级域，这是正式注册给组织和个人的唯一名称，例如www.microsoft.com中的microsoft就是微软注册的域名。

在二级域之下，组织机构还可以划分子域，使其各个分支部门都获得一个专用的名称标识，例如www.sales.microsoft.com中的sales是微软销售部门的子域名称。划分子域的工作可以一直延续下去，直到满足组织机构的管理需要为止。但是标准规定，一个域名的长度通常不超过63个字符，最多不能超过255个字符。

DNS标准还规定，域名中只能使用ASCII字符集的有限子集，包括26个英文字母（不区分大小写）和10个数字，以及连字符“-”，并且连字符不能作为子域名的第一个和最后一个字母。后来的标准对字符集有所扩大。

**参考答案**

（68）A

**试题（69）**

在网络设计阶段进行通信流量分析时可以采用简单的80/20规则，下面关于这种规则的说明中，正确的是__（69）__。

（69）A．这种设计思路可以最大限度地满足用户的远程联网需求

B．这个规则可以随时控制网络的运行状态

C．这个规则适用于内部交流较多而外部访问较少的网络

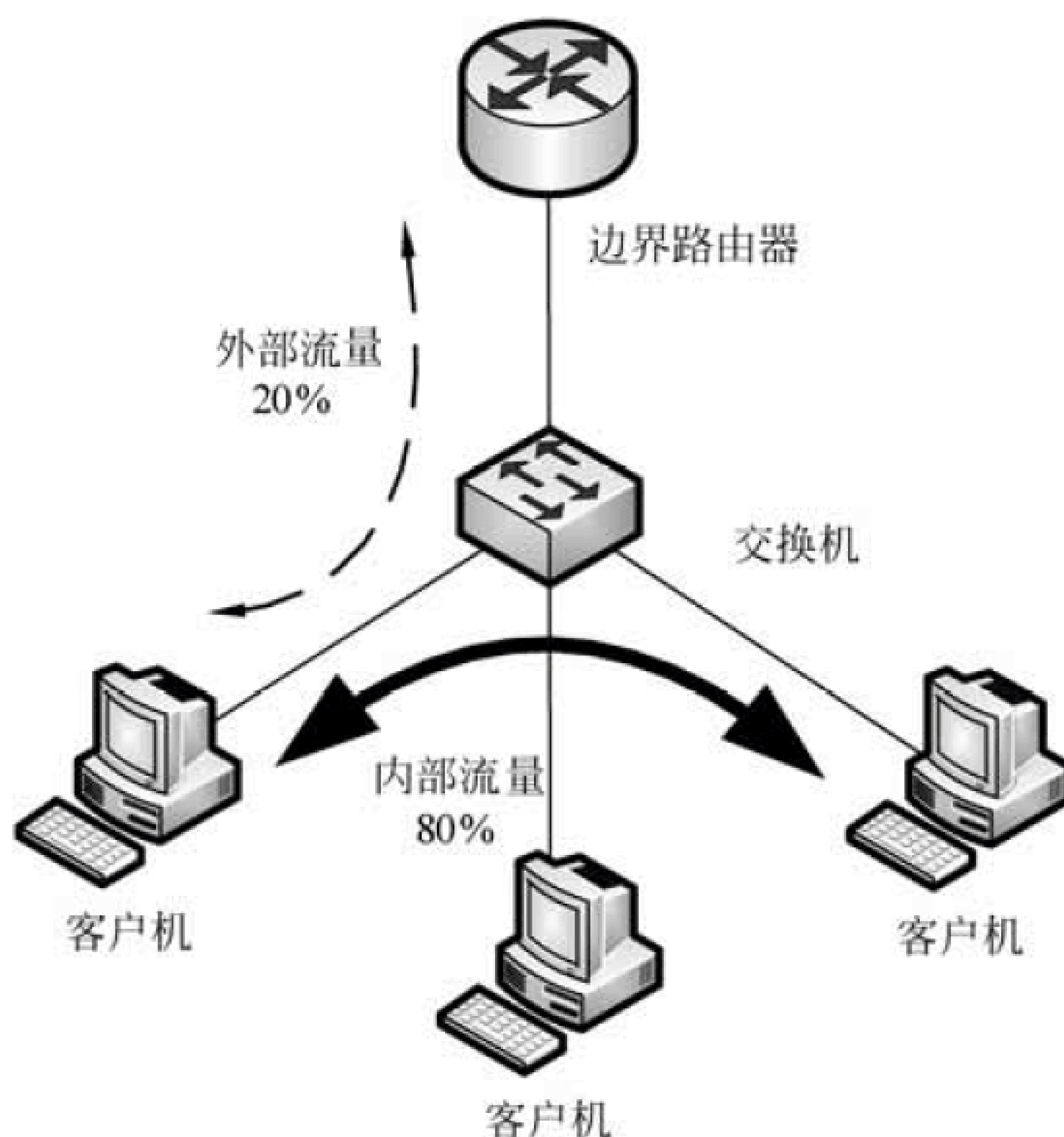
D．这个规则适用的网络允许存在具有特殊应用的网段

**试题（69）分析**

在网络规划过程中，需要根据业务需求和应用需求来计算各个信息流量的大小，并根据通信模式、通信边界的分析，确定不同信息流在网络的不同区域和区域边界上的分布情况。

对于较为简单的网络，不需要进行复杂的通信流量分析，仅采用一些简单的方法就可以确定通信流量，例如 80/20 规则等。但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。

根据 80/20 规则如下图所示，对一个网段内部的通信流量并不进行严格的计算，仅仅是根据用户和应用需求进行统计，产生网段内总的通信流量，并认为总量的 80%是在网段内部，而 20%是对网段外部的流量。




80/20 规则是一种设计思路，通过这种方式可以限制用户的不合理需求，是最优化地使用网络骨干和使用昂贵的广域网连接的一种行之有效的方法。例如，如果核心交换机容量为 100Mb/s，局域网至外部的带宽应限制在 20Mb/s 以内。

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

随着互联网络的发展，出现了另外一种通信情况，即网段内部用户之间相互访问较少，大多数通信都是对网段外部资源的访问。例如小区内计算机用户形成的局域网络，大型公司用于实现远程协同工作的工作组网络等。对于这种情况，可以采用 20/80 规则。

根据 20/80 规则，要根据用户和应用需求的统计数据产生网段内的通信总量大小，并认为总量的 20%是在网段内部的流量，而 80%是网段外部的流量。

**参考答案**

（69）C

**试题（70）**

根据用户需求选择正确的网络技术是保证网络建设成功的关键，在选择网络技术时应考虑多种因素。下面的各种考虑中，不正确的是__（70）__。

（70）A．选择的网络技术必须保证足够的带宽，使得用户能够快速地访问应用系统
B．选择网络技术时不仅要考虑当前的需求，而且要考虑未来的发展
C．越是大型网络工程，越是要选择具有前瞻性的新的网络技术
D．选择网络技术要考虑投入产出比，通过投入产出分析确定使用何种技术

**试题（70）分析**

根据用户需求选择网络技术时应考虑如下因素：

（1）通信带宽

所选择的网络技术必须保证足够的带宽，能够保证用户快速地访问应用系统。在进行选择时，不仅局限于现有的应用需求，还要适当考虑将来的带宽增长需求。

（2）技术成熟性

所选择的网络技术必须是成熟稳定的技术，有些新的网络技术在尚没有大规模投入使用时，还存在着较多不确定因素，这将会对网络建设带来很多无法估量的损失。对于大型网络工程来说，项目本身不能成为新技术的试验田。使用较为成熟、拥有较多案例的技术是明智的选择。

（3）可扩充性

网络设计的设计依据是详细的需求分析，但是在选择网络技术时，不能仅考虑当前的需求而忽视未来的发展。在大多数情况下，设计人员都会在网络带宽、数据吞吐量、用户并发数等方面的设计中预留一定的冗余量。一般来说，这个冗余量值在 70%～80%之间。

（4）高投资产出

选择网络技术的关键是投入产出比，尤其是一些借助于网络来实现营运的工程项目，只有通过投入产出分析，才能最后决定使用何种技术。

**参考答案**

（70）C

**试题（71）～（75）**

Border Gateway Protocol (BGP) is inter-autonomous system __（71）__ protocol. BGP is based on a routing method called *path vector routing*. Distance vector routing is not a good candidate for inter-autonomous system routing because there are occasions on which the route with the smallest __（72）__ count is not the preferred route. For example, we may not want a packet through an autonomous system that is not secure even though it is the shortest route. Also, distance vector

routing is unstable due to the fact that the routers announce only the number of hop counts to the destination without actually defining the path that leads to that ＿（73）＿. A router that receives a distance vector advertisement packet may be fooled if the shortest path is actually calculated through the receiving router itself. Link ＿（74）＿ routing is also not a good candidate for inter-autonomous system routing because an internet is usually too big for this routing methoD. To use link state routing for the whole internet would require each router to have a huge link state database. It would also take a long time for each router to calculate its routing ＿（75）＿ using the Dijkstra algorism.

（71）A. routing　B. switching　C. transmitting　D. receiving
（72）A. path　B. hop　C. route　D. packet
（73）A. connection　B. window　C. source　D. destination
（74）A. status　B. search　C. state　D. research
（75）A. table　B. state　C. metric　D. cost

**参考译文**

边界网关协议（BGP）是自治系统之间的路由协议。BGP 基于一种叫作通路矢量路由的路由算法。距离矢量路由算法对于自治系统之间的路由选择不是一种好方法，因为会出现一种情况，最小跳步数路由并不是所期望的路由。例如，我们不希望分组通过一个不安全的自治系统，虽然它是最短路由。同时，距离矢量路由不合适还由于下面的事实，路由器只宣布到达目标的跳步数，而没有实际定义到达那个目标的通路。如果要计算的最短通路实际上通过接收路由器本身，则接收到距离矢量公告分组的路由器就被欺骗了。对于自治系统间的路由，链路状态算法也不是好的选项，因为互联网对于这种路由方法是太大了。把链路状态算法用于整个互联网，则要求每一个路由器维护一个巨大的链路状态数据库。这就要求每一个路由器花费很长时间根据 Dijkstra 算法计算它的路由表。

**参考答案**

（71）A　（72）B　（73）D　（74）C　（75）A

# 第 10 章　2011 上半年网络工程师下午试题分析与解答

**试题一（15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业欲构建局域网，考虑到企业的很多业务依托于网络，要求企业内部用户能够高速的访问企业服务器，并且对网络的可靠性要求很高。因此，在网络的设计中，要考虑网络的冗余性，不能因为单点故障引起整个网络的瘫痪。

某网络公司根据企业需求，将网络拓扑结构设计为双核心来进行负载均衡，当其中一个核心交换机出现故障时，数据能够转换到另一台交换机上，起到冗余备份的作用。该公司给出的网络拓扑如图 1-1 所示。

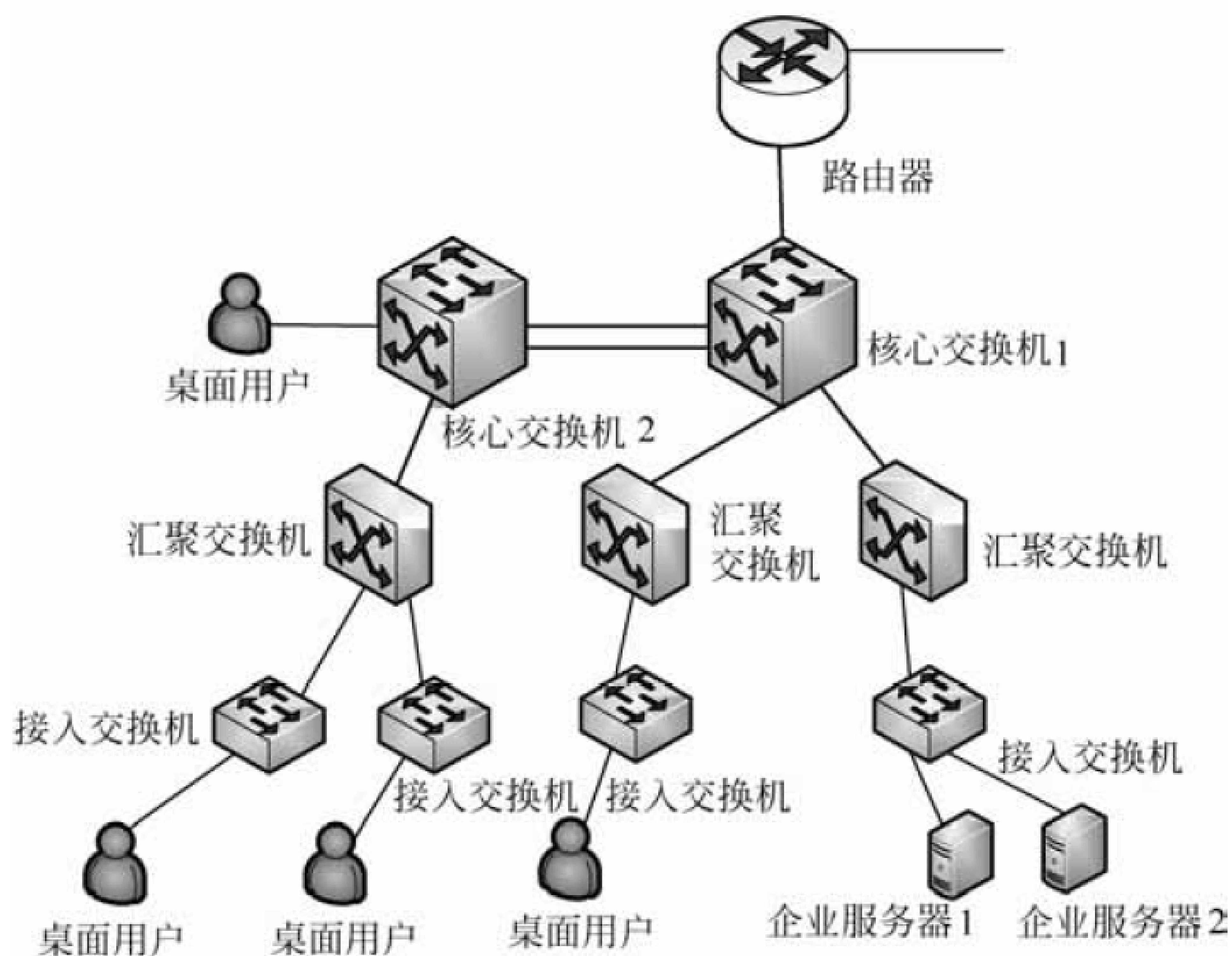



图 1-1

**【问题 1】（6 分）**

在该网络拓扑图中，请根据用户需求和设计要求，指出至少三个不合理之处，并简要说明理由。

**【问题 2】（5 分）**

该企业有部分分支机构地处其他省市，计划采用 MPLS VPN 进行网络互连，请根据

MPLS VPN 的技术原理回答以下问题：

1．MPLS 技术主要是为了提高路由器转发速率而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心就是把＿（1）＿封装在＿（2）＿数据包。

（1）、（2）备选答案：

A．IP 数据报　B．MPLS　C．TCP　D．GRE

2．MPLS VPN 承载平台上的设备主要由各类路由器组成，其中＿（3）＿是 MPLS 核心网中的路由器，这些路由器只负责依据 MPLS 标签完成数据包的高速转发，＿（4）＿是 MPLS 核心网上的边缘路由器，负责待传送数据包的 MPLS 标签的生成和弹出，还将发起根据路由建立交换标签的动作。＿（5）＿是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包。

（3）～（5）备选答案：

A．PE 路由器　B．CE 路由器　C．P 路由器

**【问题 3】（4 分）**

企业网络运行过程中会碰到各种故障。一方面，网络管理人员可以利用网络设备及系统本身提供的集成命令对网络进行故障排除，例如利用＿（6）＿命令查看系统的安装情况与网络的正常运行状况。另一方面，利用专用故障排除工具可以快速的定位故障点，例如利用＿（7）＿可以精确地测量光纤的长度、定位光纤的断点。

（6）备选答案：

A．ping　B．debug　C．show　D．tracert

（7）备选答案：

A．数字万用表　B．时域反射计

C．光时域反射计　D．网络分析仪

**试题一分析**

本题考查网络规划及网络故障排除的基本知识。

**【问题 1】**

本问题考查双核心网络结构的基本知识。双核心网络结构主要由两台核心交换设备构建局域网核心，该网络一般也是通过与核心交换机互连的路由设备接入广域网，并且路由器与两台核心交换设备之间都存在物理链路。

双核心结构一般有如下特点：

- 核心交换设备在实现上多采用三层交换机或多层交换机；
- 网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台；
- 网络中除核心交换设备之外，不存在其他的具备路由功能的设备；
- 核心交换设备之间运行特定的网关保护或负载均衡协议，例如 HSRP、VRRP、GLBP 等；

- 核心交换设备与各 VLAN 设备间可以采用 10M/100M/1000M 以太网连接；
- 网络拓扑结构可靠；
- 路由层面可以时间无缝热切换；
- 部门局域网络访问核心局域网以及相互之间多条路径选择可靠性更高；
- 在核心交换设备端口富余的前提下，部门网络接入较为方便；
- 设备投资比单核心高；
- 对核心路由设备的端口密度要求较高；
- 核心交换设备和桌面计算机之间，存在接入交换设备，接入交换设备同时和双核心存在物理连接；
- 所有服务器都直接同时连接至两台核心交换机，借助于网关保护协议，实现桌面用户对服务器的高速访问。

根据双核心结构的特点和题目要求及拓扑结构图可以判断，该网络拓扑图中的不合理之处有：

① 汇聚交换机应该分别链路连接到两个核心交换机，形成链路冗余，保证网络的可靠性。

② 两个核心交换机都应直接上联到路由器上，保证网络的可靠性。

③ 服务器应该连接到核心交换机，保证高速访问。

④ 桌面用户不应直接接入到核心交换机上，影响核心交换机性能。

**【问题 2】**

本问题考查 MPLS 技术的基本知识。

MPLS（Multi-protocol Label Switching）是多协议标签交换的简称，它用短而定长的标签来封装分组。MPLS 从各种链路层（如 PPP、ATM、帧中继、以太网等）得到链路层服务，又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持，同时还支持基于策略的约束路由，路由功能强大、灵活，可以满足各种新应用对网络的要求。

MPLS 技术主要是为了提高路由器转发速度而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心就是在 IP 数据包之外封装一个 32 比特的 MPLS 包头，MPLS 体系中的各个路由设备将根据 MPLS 包头中的标签进行转发，而不是传统方式下根据 IP 包头中的目标地址来转发；由于 MPLS 标签栈可以无限嵌套，从而提供无限的业务支持能力，而 MPLS VPN 就是一个典型的标签嵌套应用。

MPLS VPN 承载平台上的设备主要由各类路由器组成，这些路由器在 MPLS VPN 平台中的角色各不相同，分别被称为 P 设备、PE 设备、CE 设备；P（Provider Router）路由器是 MPLS 核心网中的路由器，这些路由器只负责依据 MPLS 标签完成数据包的高速转发；PE（Provider Edge Router）路由器是 MPLS 核心网上的边缘路由器，与用户的 CE 路由器互连，PE 设备负责待传送数据包的 MPLS 标签的生成和弹出，负责将数据包按

标签发送给 P 路由器或接收来自 P 路由器的含标签数据包，PE 路由器还将发起根据路由建立交换标签的动作；CE（Custom Edge）路由器是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包，CE 路由器将用户网络的信息发送给 PE 路由器，以便于在 MPLS 平台上进行路由信息的处理。

**【问题 3】**

本问题考查网络故障排除的基本知识。

1．利用网络设备及系统提供的集成命令可以监视网络并排除故障。一些常用的诊断命令有：

- show 可以用于监测系统的安装情况与网络的正常运行状况，也可以用于对故障区域的定位。
- debug 命令帮助分离协议和配置问题。
- ping 命令用于检测网络上不同设备之间的连通性。
- trace 命令可以用于确定数据包在从一个设备到另一设备直至目的地的过程中所经过的路径。

2．专用故障排除工具：

典型的排除网络故障的专用工具如下：

（1）欧姆表、数字万用表及电缆测试器。

欧姆表、数字万用表属于电缆检测工具中比较低档的一类。这类设备能够测量诸如交直流电压、电流、电阻、电容以及电缆连续性之类的参数。利用这些参数可以检测电缆的物理连通性。

（2）时域反射计与光时域反射计。

电缆检测工具中比较高档的是时域反射计（TDR）。这种设备能够快速的定位金属电缆中的断路、短路、压接、扭结、阻抗不匹配及其他问题。

对于光纤的测试则需要使用光时域反射计（OTDR）。OTDR 可以精确地测量光纤的长度、定位光纤的断裂处、测量光纤的信号衰减、测量接头或连接器造成的损耗。

（3）断接盒、智能测试盘和位/数据块错误测试器。

断接盒、智能测试盘和位/数据块错误测试器（BERT/BLERT）是用于测量 PC、打印机、调制解调器、信道服务设备/数字服务设备（CSU/DSU）以及其他外围接口数字信号的数字接口测试工具。

（4）网络监测器。

网络监测器能够持续不断地跟踪数据包在网络上的传输，能够提供任何时刻网络活动的精确描述或者一段时间内网络活动的历史记录。

（5）网络分析仪。

网络分析仪（network analyzer），也称为协议分析仪（protocol analyzer），它能够对不同协议层的通信数据进行解码，详细表示哪个层被调用（物理层、数据链路层等），以

及每个字节或者字节内容起什么作用。

**参考答案**

**【问题 1】**

1．汇聚交换机应该分别链路连接到两个核心交换机，形成链路冗余，保证网络的可靠性。

2．两个核心交换机都应直接上连到路由器上，保证网络的可靠性。

3．服务器应该连接到核心交换机，保证高速访问。

4．桌面用户不应直接接入到核心交换机上，影响核心交换机性能。

**【问题 2】**

1．（1）A．IP 数据报　（2）B．MPLS

2．（3）P 路由器　（4）PE 路由器　（5）CE 路由器

**【问题 3】**

（6）C 或 show

（7）C 或光时域反射计

**试题二（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

Linux 系统有其独特的文件系统 ext2，文件系统包括了文件的组织结构、处理文件的数据结构及操作文件的方法。可通过命令获取系统及磁盘分区状态信息，并能对其进行管理。

**【问题 1】（6 分）**

以下命令中，改变文件或所属群组的命令是__（1）__，编辑文件的命令是__（2）__，查找文件的命令是__（3）__。

（1）～（3）备选答案：

A．chmod　B．chgrp　C．vi　D．which

**【问题 2】（2 分）**

Linux 系统中，用户和应用程序可以通过__（4）__文件系统得到系统的信息，并可以改变内核的某些参数，该文件系统只存在于内存中。

（4）备选答案：

A．/proc　B．ntfs　C．/tmp　D．/etc/profile

**【问题 3】（4 分）**

在 Linux 中，分区分为主分区、扩展分区和逻辑分区，使用 fdisk-l 命令获得分区信息如下所示：

```
Disk /dev/hda:240 heads, 63 sectors, 1940 cylinders
Units = cylinders of 15120 * 512 bytes
```

| Device Boot | Start | End | Blocks | Id | System |
|---|---|---|---|---|---|
| /dev/hda | 1 | 286 | 2162128+ | c | Win95 FAT32 (LBA) |
| /dev/hda2 * | 288 | 1940 | 12496680 | 5 | Extended |
| /dev/hda5 | 288 | 289 | 15088+ | 83 | Linux |
| /dev/hda6 | 290 | 844 | 4195768+ | 83 | Linux |
| /dev/hda7 | 845 | 983 | 1050808+ | 82 | Linux swap |
| /dev/hda8 | 984 | 1816 | 6297448+ | 83 | Linux |
| /dev/hda9 | 1817 | 1940 | 937408+ | 83 | Linux |

其中，属于扩展分区的是__（5）__。

使用 df -T 命令获得信息部分如下所示：

| Filesystem | Type | 1K Blocks | Used | Available | Use% | Mounted on |
|---|---|---|---|---|---|---|
| /dev/hda6 | reiserfs | 4195632 | 2015020 | 2180612 | 49% | / |
| /dev/hda5 | ext2 | 14607 | 3778 | 10075 | 8% | /boot |
| /dev/hda9 | reiserfs | 937372 | 202368 | 735004 | 22% | /home |
| /dev/hda8 | reiserfs | 6297248 | 3882504 | 2414744 | 62% | /opt |
| Shmfs | shm | 256220 | 0 | 256220 | 0% | /dev/shm |
| /dev/hda1 | vfat | 2159992 | 1854192 | 305800 | 86% | /windows/C |

其中，不属于 Linux 系统分区的是__（6）__。

**【问题 4】（3 分）**

在 Linux 系统中，对于__（7）__文件中列出的 Linux 分区，系统启动时会自动挂载。此外，超级用户可通过__（8）__命令将分区加载到指定目录，从而该分区才在 Linux 系统中可用。

**试题二分析**

本题考查 Linux 操作系统下常用文件操作和磁盘管理。

**【问题 1】**

本问题考查对常用文件操作命令的了解程度。

**【问题 2】**

本问题考查 Linux 系统中/proc 文件系统的基本概念。

**【问题 3】**

本问题考查 Linux 系统分区的基础知识。

**【问题 4】**

本问题考查对 Linux 系统中/etc/fstab 配置文件及分区加载命令的熟悉程度。

**参考答案**

**【问题 1】**

（1）B　或 chgrp

（2）C　或 vi

（3）D 或 which

**【问题 2】**

（4）A 或 /proc

**【问题 3】**

（5）/dev/hda2

（6）/dev/hda1

**【问题 4】**

（7）/etc/fstab

（8）mount

**试题三（15 分）**

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

某网络拓扑结构如图 3-1 所示，网络 1 和网络 2 的主机均由 DHCP_Server 分配 IP 地址。FTP_Server 的操作系统为 Windows Server 2003，Web_Server 的域名为 www.softexamtest.com。

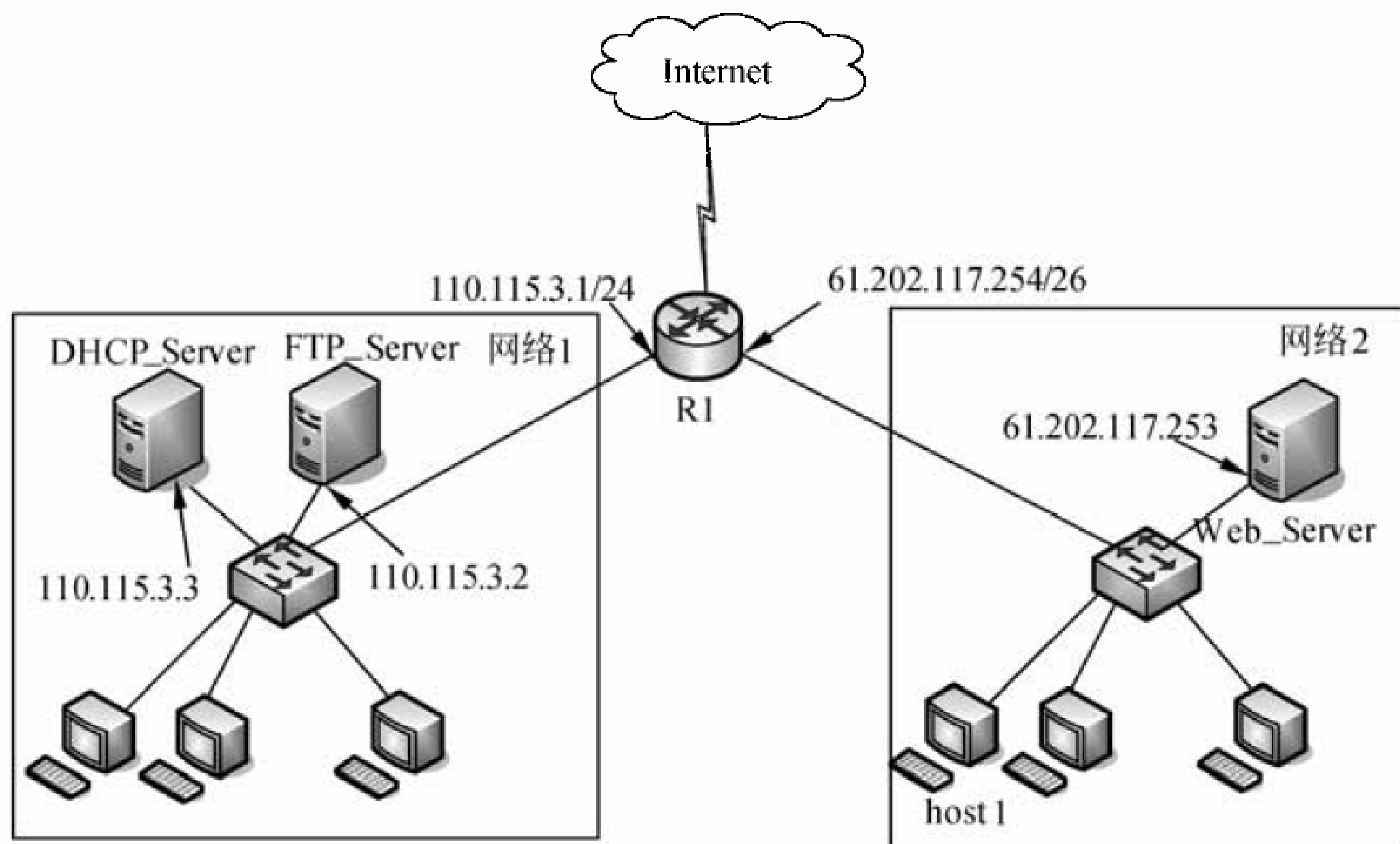



图 3-1

**【问题 1】（4 分）**

DHCP_Server 服务器必须包含的 IP 地址范围为＿（1）＿和＿（2）＿。

**【问题 2】（2 分）**

若在 host1 上运行 ipconfig 命令，获得如图 3-2 所示结果，host1 能正常访问 Internet 吗？说明原因。

**【问题 3】（3 分）**

若 host1 成功获取 IP 地址后，在访问 http://www.abc.com 网站时，总是访问到

www.softexamtest.com，而同一网段内的其他客户端访问该网站正常。在 host1 的 C:\WINDOWS\system32\drivers\etc 目录下打开____（3）____文件，发现其中有如下两条记录：

```
127.0.0.1       localhost
____（4）____    www.abc.com
```

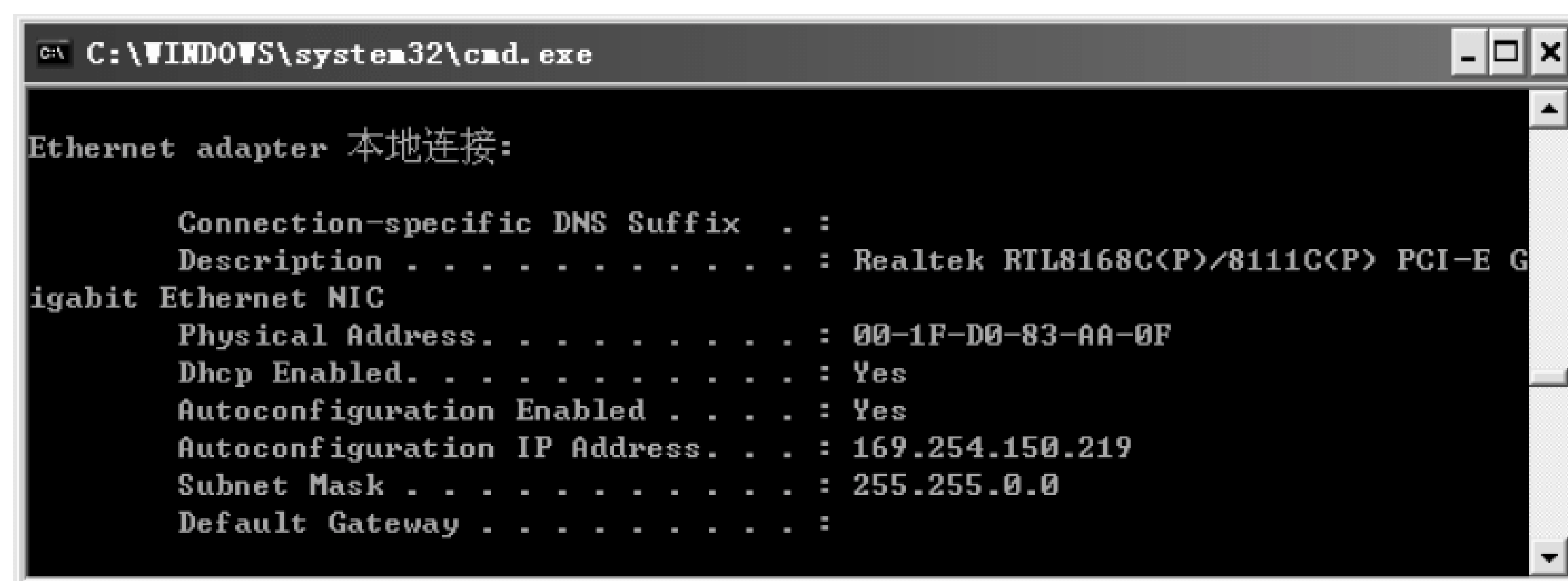



图 3-2

在清除第 2 条记录后关闭文件，重启系统后 host1 访问 http://www.abc.com 网站正常。请填充空（4）处空缺内容。

**【问题 4】（2 分）**

在配置 FTP_server 时，图 3-3 中“IP 地址”文本框中应填入____（5）____。

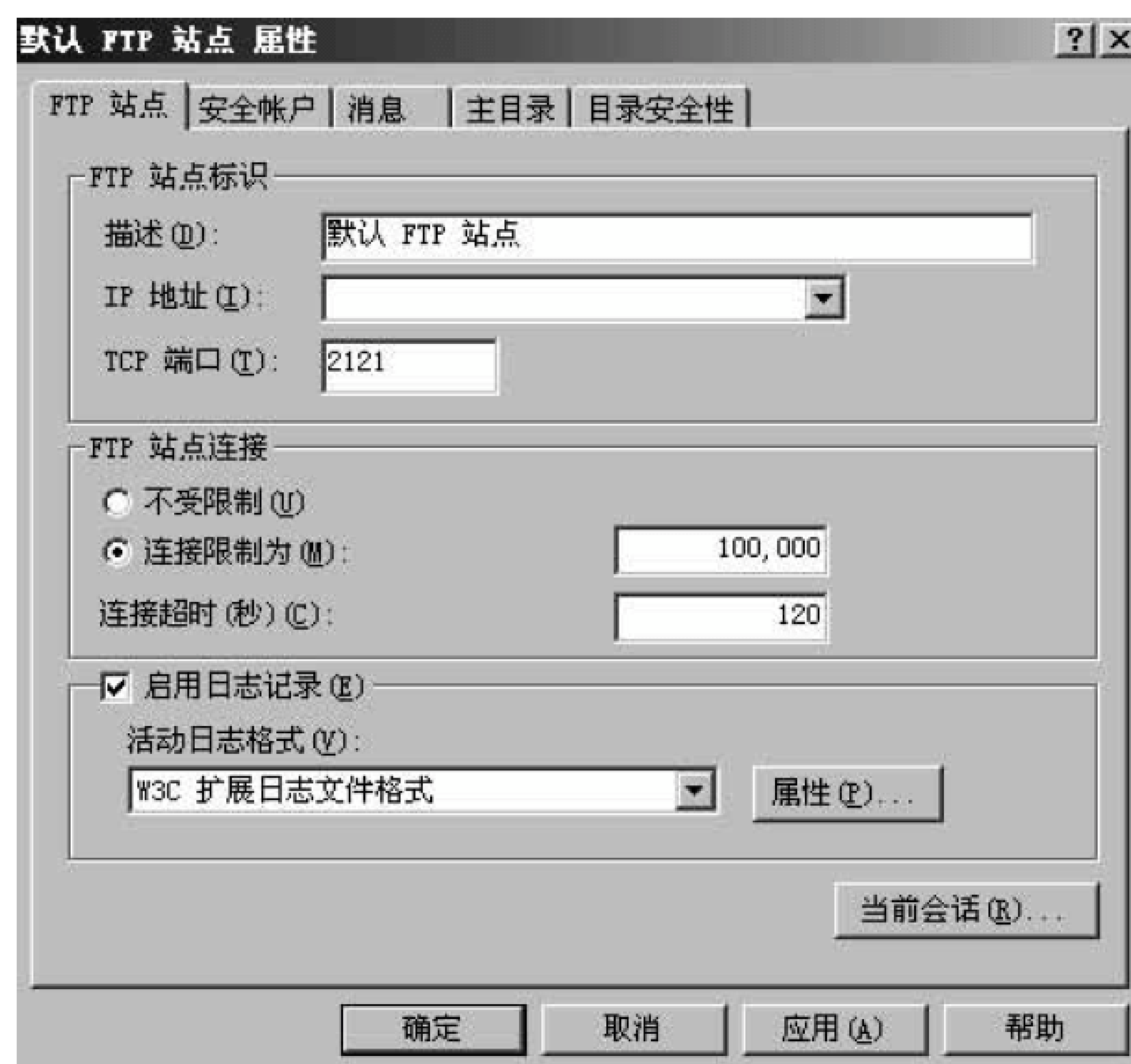



图 3-3

**【问题 5】（4 分）**

若 FTP 配置虚拟目录为 pcn，虚拟目录配置如图 3-4 与图 3-5 所示。

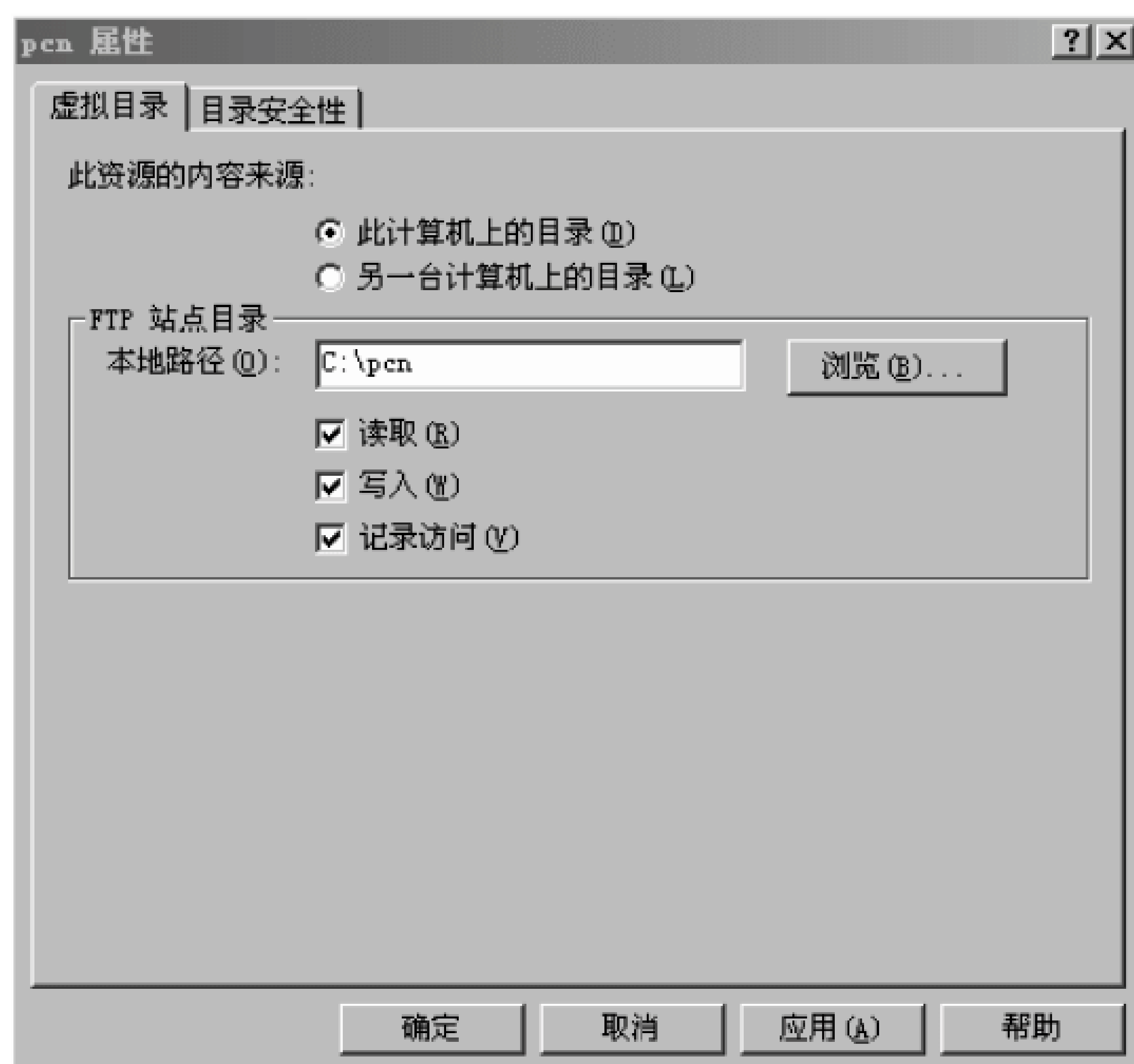



图 3-4




图 3-5

根据以上配置，哪些主机可访问该虚拟目录？访问该虚拟目录的命令是＿（6）＿。

**试题三解析**

本题考查内容为 Windows Server 2003 中 DHCP 和 FTP 服务器配置。

**【问题 1】**

DHCP_Server 服务器需为网络 1 和网络 2 的主机分配 IP 地址。由网络 1 和网络 2 的网关分别为 110.115.3.1/24 与 61.202.117.254/26 可知，网络 1 包含的可用的 IP 地址范围为 110.115.3.1～110.115.3.254，网络 2 可用的 IP 地址范围为 61.202.117.193～61.202.117.254，除去网络 1 和网络 2 中已用的服务器和路由器接口地址，能分配的地址区间为 110.115.3.4～110.115.3.254 和 61.202.117.193～61.202.117.252。

**【问题 2】**

自动专用 IP 地址（Automatic Private IP Address，APIPA）是当客户机无法从 DHCP 服务器中获得 IP 地址时自动配置的地址。IPv4 地址前缀 169.254/16 已经被 IANA 注册为 APIPA 专用（RFC 3927）。

当网络中的 DHCP 服务器失效，或者由于网络故障而找不到 DHCP 服务器时，这个功能开始生效，使得客户机可以在一个小型局域网中运行，与其他自动或手工获得 APIPA 地址的计算机进行通信。其实 APIPA 的主要用途是为了移动计算使用的，两个笔记本电脑用户之间可以通过 APIPA 地址直接通信，而不需要其他网络连接的支持。

host1 的 IP 地址为 169.254.150.219，故不能正常访问 Internet。

**【问题 3】**

host1 访问 http://www.abc.com 网站时总是访问到 www.softexamtest.com，而同一网段内的其他客户端访问该网站正常。可知在 host1 本地 hosts 文件中应该存在一条 DNS

记录，把域名 www.abc.com 映射到 www.softexamtest.com 所对应的 IP 地址，故解决该故障的方法是打开 host1 的 hosts 文件，清除该记录，重启系统。

hosts 文件中记录的格式为：IP 地址 域名，故空（3）处应填入 hosts，空（4）处应填入 61.202.117.253。

**【问题 4】**

“IP 地址”文本框中应填入的是该 FTP 站点对应的 IP 地址，故空（5）处应填入 110.115.3.2。

**【问题 5】**

图中显示除了添加上的 IP 地址可以访问虚拟目录 pcn，其他均拒绝访问，故具有访问权限的只有主机 110.115.3.10。由配置方式的不同，采用带虚拟目录名和不带虚拟目录名两种方式均可访问该站点，再加上配置图中已经指明 TCP 的端口号为 2121，故访问该虚拟目录的命令为 ftp://110.115.3.2:2121 或 ftp://110.115.3.2:2121/pcn 均可。

**参考答案**

**【问题 1】**

（1）110.115.3.4～110.115.3.254

（2）61.202.117.193～61.202.117.252（（1）、（2）可互换）

**【问题 2】**

不能。由于该主机地址是自动专用 IP 地址（APIPA），即当客户机无法从 DHCP 服务器中获得 IP 地址时自动配置的地址。

**【问题 3】**

（3）hosts

（4）61.202.117.253

**【问题 4】**

（5）110.115.3.2

**【问题 5】**

只有 110.115.3.10 可访问该虚拟目录。

（6）ftp://110.115.3.2:2121 或 ftp://110.115.3.2:2121/pcn

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司两分支机构之间的网络配置如图 4-1 所示，为保护通信安全，在路由器 router-a 和 router-b 上配置 IPSec 安全策略，对 192.168.8.0/24 网段和 192.168.9.0/24 网段之间的数据进行加密处理。

**【问题 1】（3 分）**

为建立两分支机构之间的通信，请完成下面的路由配置命令。

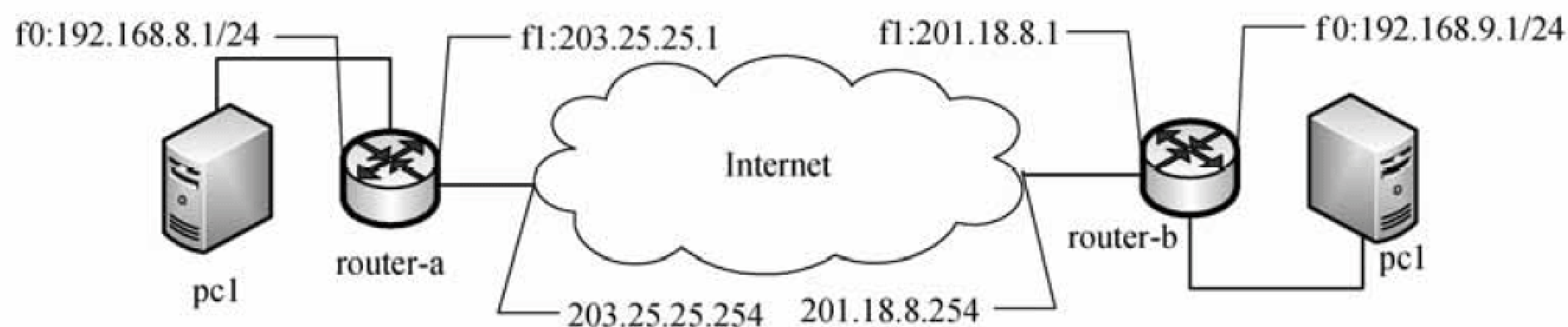



图 4-1

```
router-a (config) #ip route  0.0.0.0  0.0.0.0  (1)
router-b (config) #ip route  0.0.0.0  0.0.0.0  (2)
```

【问题 2】(3 分)

下面的命令是在路由器 router-a 中配置 IPSec 隧道。请完成下面的隧道配置命令。

```
router-a(config)# crypto tunnel tun1            (设置 IPSec 隧道名称为 tun1)
router-a(config-tunnel)# peer address  (3)      (设置隧道对端 IP 地址)
router-a(config-tunnel)# local address  (4)     (设置隧道本端 IP 地址)
router-a(config-tunnel)# set auto-up            (设置为自动协商)
router-a(config-tunnel)# exit                   (退出隧道设置)
```

【问题 3】(3 分)

router-a 与 router-b 之间采用预共享密钥“12345678”建立 IPSec 安全关联，请完成下面配置命令。

```
router-a(config)# crypt  ike key 12345678 address  (5)
router-b(config)# crypt  ike key 12345678 address  (6)
```

【问题 4】(3 分)

下面的命令在路由器 router-a 中配置了相应的 IPSec 策略，请说明该策略的含义。

```
router-a(config)# crypto policy p1
router-a(config-policy)# flow 192.168.8.0 255.255.255.0 192.168.9.0
255.255.255.0
ip tunnel tun1
router-a(config-policy)#exit
```

【问题 5】(3 分)

下面的命令在路由器 router-a 中配置了相应的 IPSec 提议，该提议表明：IPSec 采用 ESP 报文，加密算法采用 (7) ，认证算法采用 (8) 。

```
router-a(config)# crypto ipsec proposal secp1
router-a(config-ipsec-prop)# esp 3des sha1
router-a(config-ipsec-prop)# exit
```

**试题四分析**

本题考查考生在路由器上配置 IPSec 安全策略的实际操作能力。

**【问题 1】**

本问题考查如何在两个路由器上配置默认路由，从图 4-1 中可以得到 router-a 的默认路由是 203.25.25.254，router-b 的默认路由是 201.18.8.254。

**【问题 2】**

本问题考查如何在 router-a 上配置 IPSec 隧道，对端 IP 地址应该是 router-b 的 f1 口地址 201.18.8.1，本地地址是 router-b 的 f1 口地址 203.25.25.1。

**【问题 3】**

本问题考查如何在 router-a 与 router-b 之间预设共享密钥，address 后面是对端的 id，默认是对端的 IP 地址。

**【问题 4】**

本问题考查如何配置相应的 IPSec 策略，该策略说明从 192.168.8.0/24 子网到 192.168.9.0/24 子网的所有 IP 报文经由 IPSec 隧道到达。

**【问题 5】**

本问题考查如何配置 IPSec 提议，提议表明 IPSec 采用 ESP 报文，加密算法采用 3DES，认证算法采用 SHA-1。

**参考答案**

**【问题 1】**

（1）203.25.25.254

（2）201.18.8.254

**【问题 2】**

（3）201.18.8.1

（4）203.25.25.1

**【问题 3】**

（5）201.18.8.1

（6）203.25.25.1

**【问题 4】**

从 192.168.8.0/24 子网到 192.168.9.0/24 子网的所有 IP 报文经由 IPSec 隧道到达。

**【问题 5】**

（7）3DES

（8）SHA-1

**试题五（15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某单位网络的拓扑结构示意图如图 5-1 所示。该网络采用 RIP 协议，要求在 R2 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问网络 192.168.10.0/24，在 R3 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，但允许其访问其他服务器。

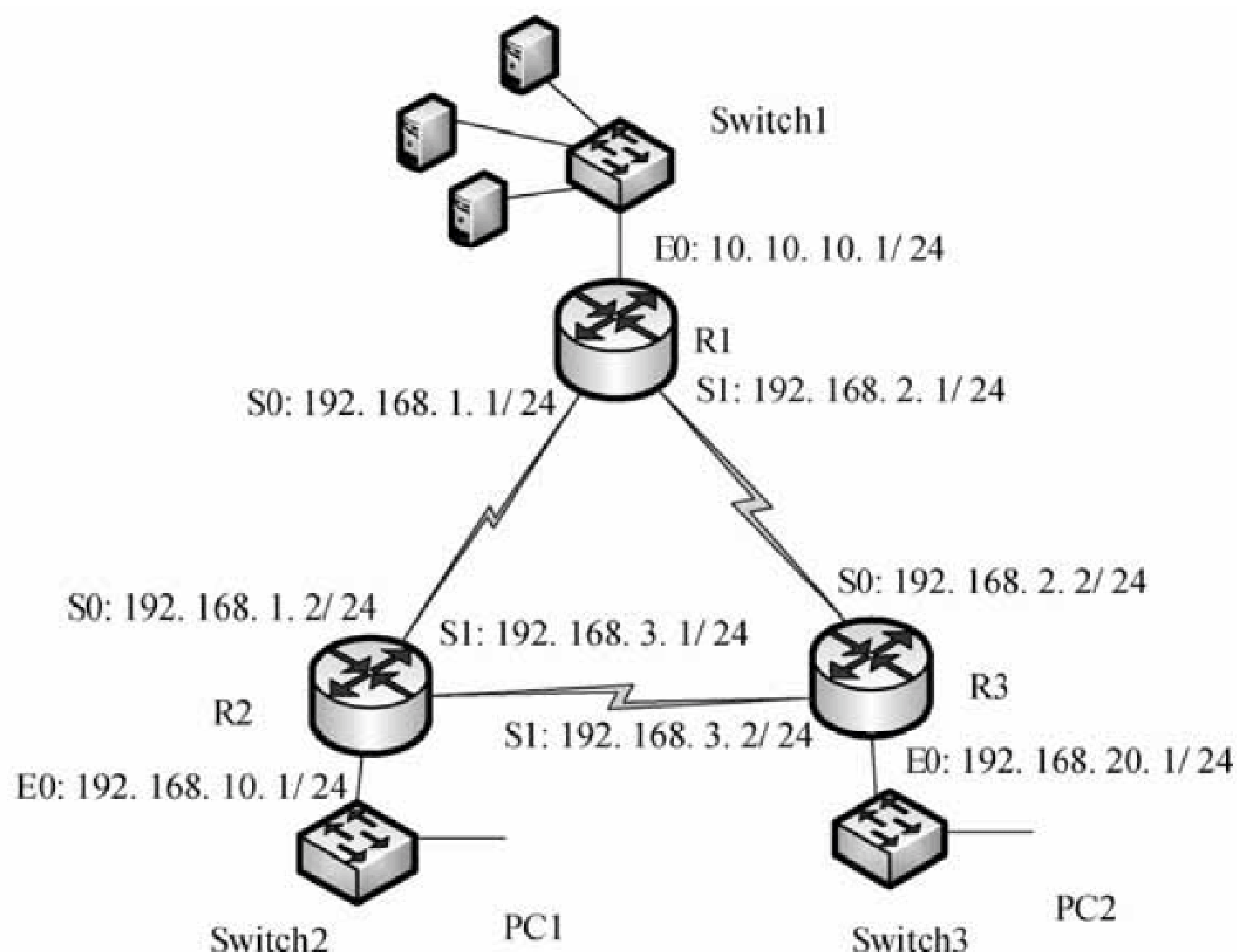



图 5-1

【问题 1】（4 分）

下面是路由器 R1 的部分配置，请根据题目要求，完成下列配置。

```
……
R1(config)# interface Serial0
R1(config-if)# ip address ___(1)___ ___(2)___
R1 (config)#ip routing
R1 (config)#___(3)___                    (进入 RIP 协议配置子模式)
R1 (config-router)#___(4)___             (声明网络 192.168.1.0/24)
……
```

【问题 2】（6 分）

下面是路由器 R2 的部分配置，请根据题目要求，完成下列配置。

```
R2# config t
R2(config)# access-list 50 deny 192.168.20.0  0.0.0.255
R2(config)# access-list 50 permit  any
```

```
R2(config)# interface ___(5)___
R2(config-if)# ip access-group ___(6)___ ___(7)___
```

**【问题 3】（5 分）**

1．下面是路由器 R3 的部分配置，请根据题目要求，完成下列配置。（2 分）

```
R3(config)#access-list 110 deny ___(8)___ 192.168.20.0 0.0.0.255 10.10.10.0
0.0.0.255 eq ___(9)___
R3(config)# access-list 110 permit ip any any
```

2．上述两条语句次序是否可以调整？简单说明理由。（3 分）

**试题五分析**

本题考查路由器 RIP 配置及 ACL 配置的知识。

**【问题 1】**

本问题考查路由器的 RIP 协议的配置及路由器接口地址的基本配置操作。根据题目拓扑结构图可知，路由器 R1 的 S0 口地址为 192.168.1.1/24；所以其配置如下：

```
……
R1(config)# interface Serial0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1 (config)#ip routing
R1 (config)# router rip                    （进入 RIP 协议配置子模式）
R1 (config-router)# network 192.168.1.0    （声明网络 192.168.1.0/24）
……
```

**【问题 2】**

本问题考查标准 ACL 的基本配置。根据题目要求，要求在 R2 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问网络 192.168.10.0/24。根据题目拓扑结构图可知，该 ACL 应该配置在 R2 的 E0 口上，方向为 out。所以配置命令如下：

```
R2# config t
R2(config)# access-list 50 deny 192.168.20.0  0.0.0.255
                        （创建 ACL50 拒绝源 192.168.20.0/24 数据）
R2(config)# access-list 50 permit  any
R2(config)# interface fastethernet 0/0        （进入端口 E0 配置模式）
R2(config-if)# ip access-group 50  out        （激活 ACL 50）
```

**【问题 3】**

本问题考查扩展 ACL 的基本配置。

1．根据题目要求，在 R3 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，但允许其访问其他服务器。对于 TCP 和 UDP 协议，扩展 ACL 配置命令的格式如下：

```
Router(config)# access-list 100-199|2000-2699 permit|deny tcp|udp
source_address source_wildcard_mask [operator source_port_#]
destination_address destination_wildcard_mask [operator destination_port_#]
[established] [log]
```

所以，路由器 R3 配置如下：

```
……
R3(config)# access-list 110 deny tcp 192.168.20.0 0.0.0.255 10.10.10.0
0.0.0.255 eq www _
R3(config)# access-list 110 permit ip any any
```

2．上述两条语句次序不可以调整。因为路由器对 ACL 语句的处理规则如下：

- 一旦发现匹配的语句，就不再处理列表中的其他语句，所以语句的排列顺序非常重要；
- 如果整个列表中没有匹配的语句，则分组被丢弃。

在本例中，如果次序调整，则语句 access-list 110 permit ip any any 将放行所有数据，包括网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，这样语句 access-list 110 deny tcp 192.168.20.0 0.0.0.255 10.10.10.0 0.0.0.255 eq www 将失去作用。

**参考答案**

**【问题 1】**

（1）192.168.1.1

（2）255.255.255.0

（3）router rip

（4）network 192.168.1.0

**【问题 2】**

（5）fastethernet 0/0（或 ethernet 0/0）

（6）50

（7）out

**【问题 3】**

1．（8）tcp （9）www 或 80

2．不可以调整次序，acl 执行顺序是自上而下，一旦次序调整后，原第一条规则失效。

# 第 11 章　2011 下半年网络工程师上午试题分析与解答

**试题（1）**

若某条无条件转移汇编指令采用直接寻址，则该指令的功能是将指令中的地址码送入__（1）__。

（1）A．PC（程序计数器）　　B．AR（地址寄存器）
　　C．AC（累加器）　　D．ALU（算术逻辑运算单元）

**试题（1）分析**

本题考查指令系统基础知识。

直接寻址是指操作数存放在内存单元中，指令中直接给出操作数所在存储单元的地址。而跳转指令中的操作数即为要转向执行的指令地址，因此，应将指令中的地址码送入程序计数器（PC），以获得下一条指令的地址，从而实现程序执行过程的自动控制功能。

**参考答案**

（1）A

**试题（2）**

若某计算机系统的 I/O 接口与主存采用统一编址，则输入输出操作是通过__（2）__指令来完成的。

（2）A．控制　　B．中断　　C．输入输出　　D．访存

**试题（2）分析**

本题考查计算机系统输入输出系统基础知识。

常用的 I/O 接口编址方法有两种：一是与内存单元统一编址，二是单独编址。

与内存单元统一编址方式下，是将 I/O 接口中有关的寄存器或存储部件看作存储器单元，与主存中的存储单元统一编址。这样，内存地址和接口地址统一在一个公共的地址空间里，对 I/O 接口的访问就如同对主存单元的访问一样，可以用访问内存单元的指令访问 I/O 接口。

I/O 接口单独编址是指通过设置单独的 I/O 地址空间，为接口中的有关寄存器或存储部件分配地址码，需要设置专门的 I/O 指令进行访问。这种编址方式的优点是不占用主存的地址空间，访问主存的指令和访问接口的指令不同，在程序中容易使用和辨认。

**参考答案**

（2）D

**试题（3）**

在程序的执行过程中，Cache 与主存的地址映像由__（3）__。

（3）A．专门的硬件自动完成　　B．程序员进行调度

C．操作系统进行管理　　D．程序员和操作系统共同协调完成

**试题（3）分析**

本题考查存储系统基础知识。

高速缓存（Cache）的出现主要有两个因素：首先是由于 CPU 的速度和性能提高很快而主存速度较低且价格高，其次就是程序执行的局部性特点。因此，才将速度比较快而容量有限的静态存储器芯片构成 Cache，以尽可能发挥 CPU 的高速度。因此，必须用硬件来实现 Cache 的全部功能。

**参考答案**

（3）A

**试题（4）**

总线复用方式可以__（4）__。

（4）A．提高总线的传输带宽　　B．增加总线的功能

C．减少总线中信号线的数量　　D．提高 CPU 利用率

**试题（4）分析**

本题考查总线基础知识。

总线是一组能为多个部件分时共享的信息传送线，用来连接多个部件并为之提供信息交换通路，通过总线复用方式可以减少总线中信号线的数量，以较少的信号线传输更多的信息。

**参考答案**

（4）C

**试题（5）**

确定软件的模块划分及模块之间的调用关系是__（5）__阶段的任务。

（5）A．需求分析　　B．概要设计　　C．详细设计　　D．编码

**试题（5）分析**

本题考查软件工程中的软件开发过程和软件开发阶段的基础知识。

需求分析确定软件要完成的功能及非功能性要求；概要设计将需求转化为软件的模块划分，确定模块之间的调用关系；详细设计将模块进行细化，得到详细的数据结构和算法；编码根据详细设计进行代码的编写，得到可以运行的软件，并进行单元测试。

**参考答案**

（5）B

**试题（6）**

利用结构化分析模型进行接口设计时，应以<u>（6）</u>为依据。

（6）A. 数据流图　　B. 实体-关系图　　C. 数据字典　　D. 状态-迁移图

**试题（6）分析**

本题考查结构化分析与设计基础知识。

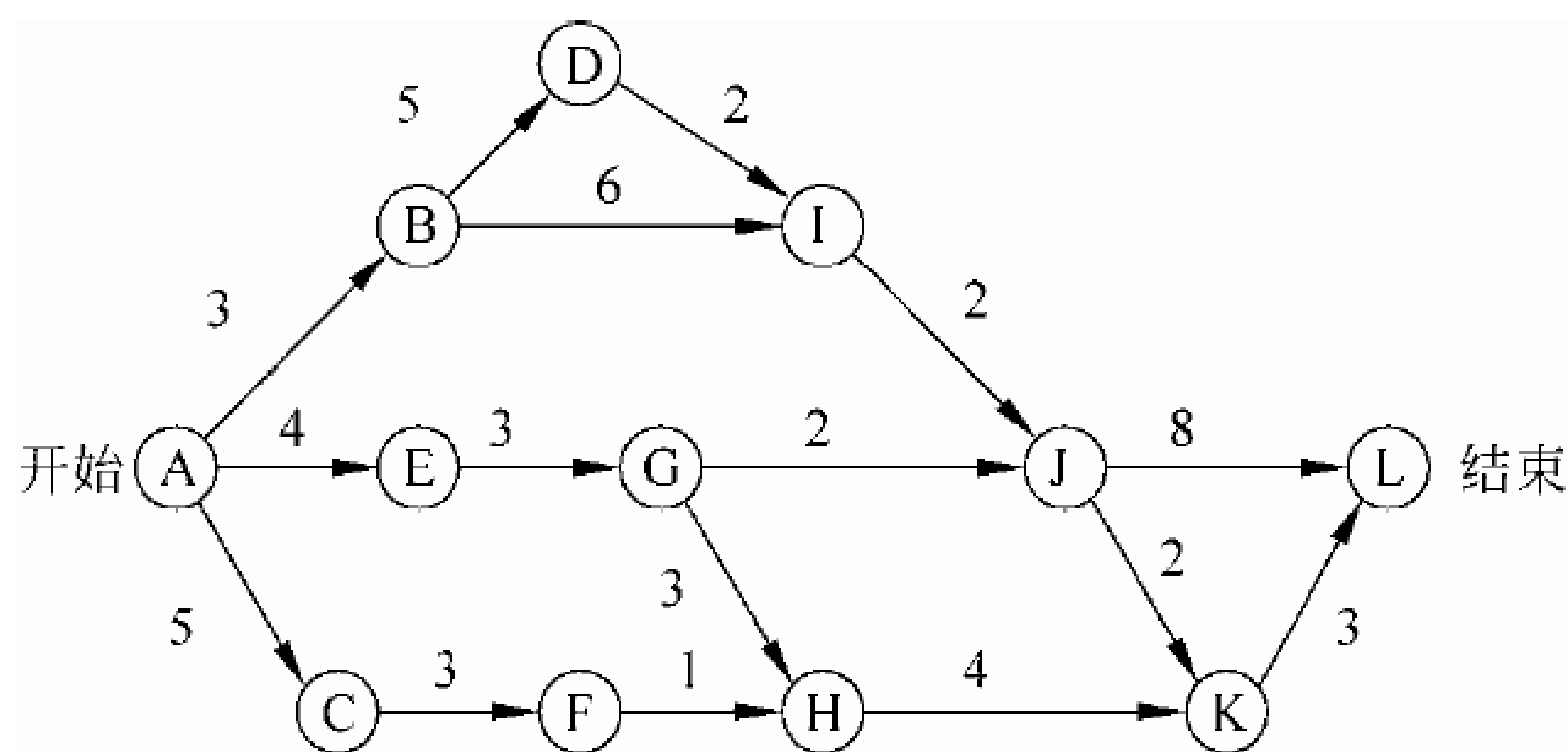
软件设计必须依据软件的需求来进行，结构化分析的结果为结构化设计提供了最基本的输入信息，其关系为：根据加工规格说明和控制规格说明进行过程设计；根据数据字典和实体关系图进行数据设计；根据数据流图进行接口设计；根据数据流图进行体系结构设计。

**参考答案**

（6）A

**试题（7）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的值表示完成活动所需要的时间，则关键路径长度为<u>（7）</u>。




（7）A. 20　　B. 19　　C. 17　　D. 16

**试题（7）分析**

本题考查软件项目管理的相关知识。

关键路径是从开始到结束的最长路径，也是完成项目所需要的最短时间。根据上述活动图，路径 A-B-D-I-J-L 是关键路径，其长度为 20。

**参考答案**

（7）A

**试题（8）、（9）**

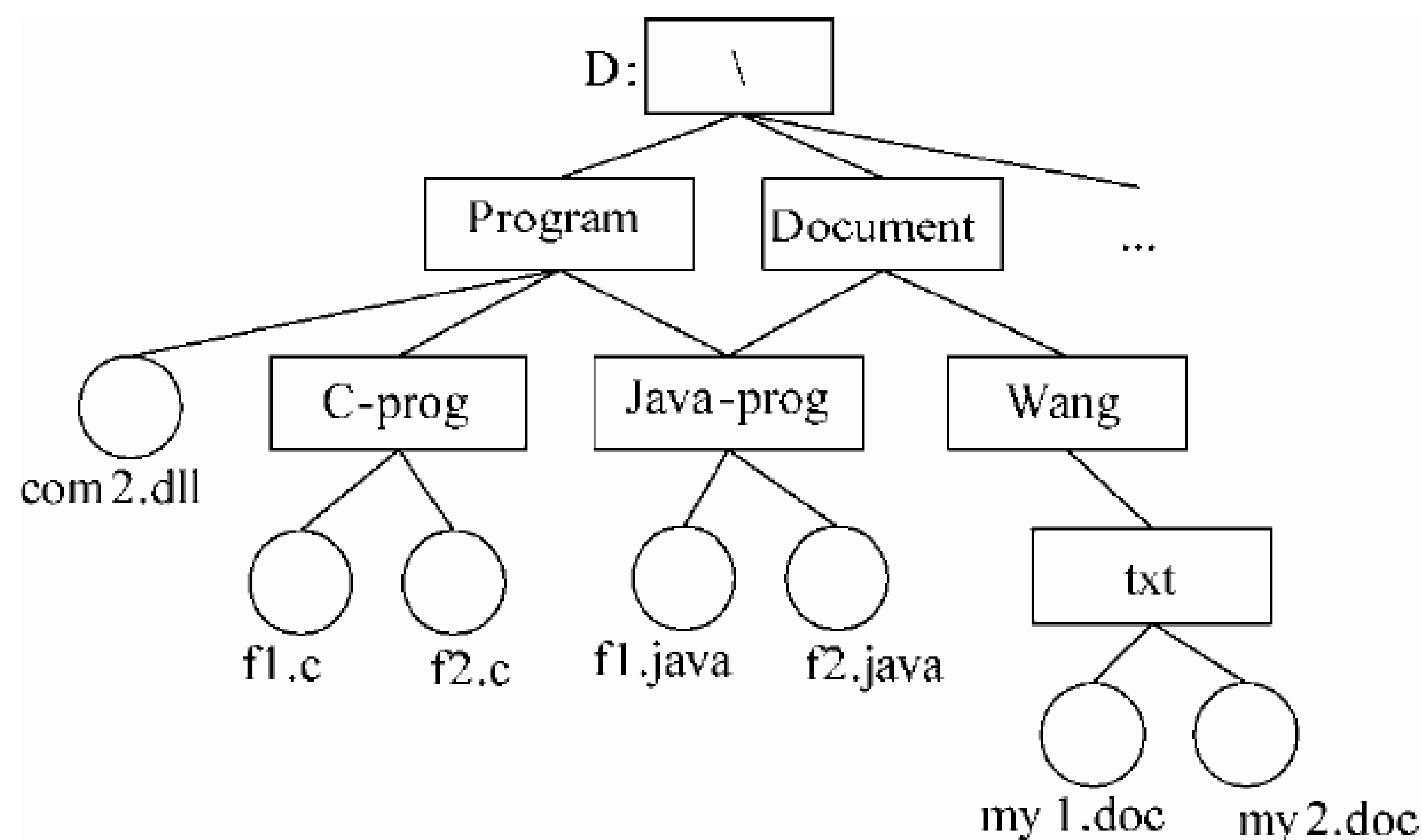
若某文件系统的目录结构如下图所示，假设用户要访问文件 f1.java，且当前工作目录为 Program，则该文件的全文件名为<u>（8）</u>，其相对路径为<u>（9）</u>。

（8）A. f1.java　　B. \Document\Java-prog\f1.java

C. D:\Program\Java-prog\f1.java　　D. \Program\Java-prog\f1.java

（9）A. Java-prog\　　B. \Java-prog\

C. Program\Java-prog　　D. \Program\Java-prog\




**试题（8）、（9）分析**

文件的全文件名应包括盘符及从根目录开始的路径名，所以从题图可以看出文件 f1.java 的全文件名为 D:\Program\Java-prog\f1.java。

文件的相对路径是当前工作目录下的路径名，所以从题图可以看出文件 f1.java 的相对路径名为 Java-prog\。

**参考答案**

（8）C　（9）A

**试题（10）**

__（10）__指可以不经著作权人许可，无需支付报酬，使用其作品。

（10）A．合理使用　　B．许可使用

C．强制许可使用　　D．法定许可使用

**试题（10）分析**

本题考查知识产权方面的基础知识。

合理使用是指在特定的条件下，法律允许他人自由使用享有著作权的作品而不必征得著作权人的同意，也不必向著作权人支付报酬，但应当在指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利的情况下对著作权人的作品进行使用。

许可使用是指著作权人将自己的作品以一定的方式、在一定的地域和期限内许可他人使用，并由此获得经济利益。

强制许可使用是指在一定条件下，作品的使用者基于某种正当理由需要使用他人已发表的作品，经申请由著作权行政管理部门授权即可使用该作品，无需征得著作权人同意，但应向其支付报酬。

法定许可是指除著作权人声明不得使用外，使用人在未经著作权人许可的情况下，向著作权人支付报酬，指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利。

**参考答案**

（10）A

**试题（11）**

两个自治系统（AS）之间的路由协议是__（11）__。

（11）A. RIP　　B. OSPF　　C. BGP　　D. IGRP

**试题（11）分析**

自治系统（AS）是由一个管理部门控制的一组网络。自治系统用 16 位号码来唯一地标识。因特网地址授权机构（Internet Assigned Numbers Authority，IANA）指定了各个地区的注册机构负责 AS 号码的分配。在 AS 内部采用相同的路由技术，实现统一的路由策略，不同的 AS 采用的路由技术和路由策略可以不同。内部网关协议（IGP）用于在自治系统内部交换路由信息，例如 RIP、OSPF 都是内部网关协议。外部网关协议（EGP）用于在两个自治系统之间交换路由信息，边界网关协议（Border Gateway Protocol，BGP）是现在广泛使用的外部网关协议。

**参考答案**

（11）C

**试题（12）**

一个以太网交换机，读取整个数据帧，对数据帧进行差错校验后再转发出去，这种交换方式称为__（12）__。

（12）A. 存储转发交换　　B. 直通交换

C. 无碎片交换　　D. 无差错交换

**试题（12）分析**

根据交换方式可以把交换机划分为 3 种：

① 存储转发交换（Store and Forward）：交换机对输入的数据包先进行缓存、验证、碎片过滤，然后再进行转发。这种交换方式延时大，但是可以提供差错校验，并支持不同速度的输入/输出端口间的交换（非对称交换），是交换机的主流工作方式。

② 直通式交换（Cut-through）：直通式交换机在输入端口扫描到目标地址后立即开始转发。这种交换方式的优点是延迟小、交换速度快。其缺点是没有检错能力；不能实现非对称交换；并且当交换机的端口增加时，交换矩阵实现起来比较困难。

③ 碎片过滤式交换（Fragment Free）：也叫做无碎片交换，这是介于直通式和存储转发式之间的一种交换方式。这种交换机在开始转发前先检查数据包的长度是否够 64 个字节，如果小于 64 字节，说明是冲突碎片，则丢弃之；如果大于 64 字节，则转发该数据包。这种转发方式的处理速度介于前两者之间，被广泛应用于中低档交换机之中。

**参考答案**

（12）A

**试题（13）**

以下关于光纤通信的叙述中，正确的是__（13）__。

（13）A. 多模光纤传输距离远，而单模光纤传输距离近

B．多模光纤的价格便宜，而单模光纤的价格较贵

C．多模光纤的包层外径较粗，而单模光纤的包层外径较细

D．多模光纤的纤芯较细，而单模光纤的纤芯较粗

**试题（13）分析**

光纤分为单模光纤和多模光纤。单模光纤（Single Mode Fiber）采用激光二极管作为光源，波长分为 1310nm 和 1550nm 两种。单模光纤的纤芯直径为 8.3μm，包层外径为 125μm，可表示为 8.3/125μm。单模光纤色散很小，适用于远程通信。如果希望支持万兆传输，而且距离较远，应考虑采用单模光缆。

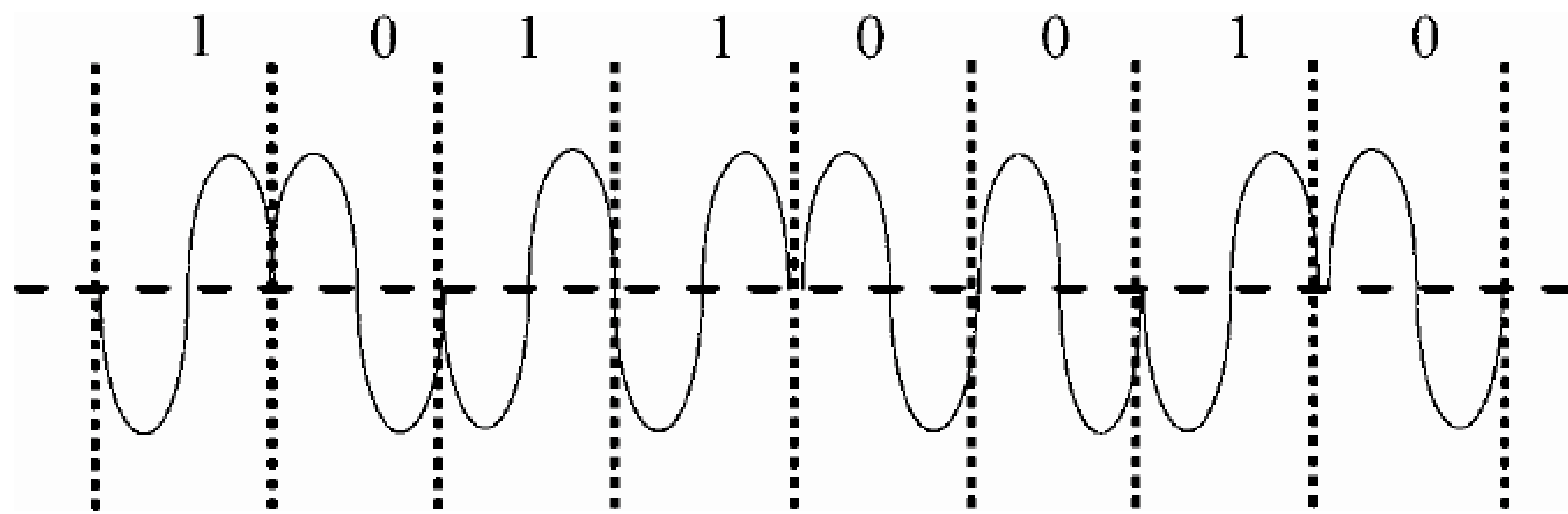
多模光纤（Multi Mode Fiber）采用发光二极管作为光源，波长分为 850nm 和 1300nm 两种。多模光纤的纤芯较粗，有 50μm 和 62.5μm 两种，包层外径 125μm，分别表示为 50/125μm 和 62.5/125μm。多模光纤可传多种模式的光，如果采用折射率突变的纤芯材料，则这种光纤称为多模突变型光纤；如果采用折射率渐变的纤芯材料，则这种光纤称为多模渐变型光纤。多模光纤的色散较大，限制了传输信号的频率，而且随距离的增加这种限制会更加严重。所以多模光纤传输的距离比较近，一般只有几千米。但是多模光纤比单模光纤价格便宜。对传输距离或数据速率要求不高的场合可以选择多模光缆。

**参考答案**

（13）B

**试题（14）**

可以用数字信号对模拟载波的不同参量进行调制，下图所示的调制方式称为<u>（14）</u>。




（14）A．ASK　　B．FSK　　C．PSK　　D．DPSK

**试题（14）分析**

数字信号只有有限个离散值，使用数字信号对载波进行调制的方式称为键控（Keying），分为幅度键控（ASK）、频移键控（FSK）和相移键控（PSK）。

幅度键控可以通过乘法器和开关电路来实现，在数字信号为“1”时电路接通，此时信道上有载波出现；数字信号为“0”时电路被关断，此时信道上无载波出现。在接收端可以根据载波的有无还原出数字信号的“1”和“0”。调幅技术实现简单，但抗干扰性能较差，在数据通信中已经很少使用了。

频移键控是利用两个不同频率（$f_1$ 和 $f_2$）的载波信号分别代表数字信号“1”和“0”，即用数字信号“1”和“0”来控制两个不同频率的振荡源交替输出。这种调制技术抗干

扰性能好，但占用带宽较大，频带利用率低，主要用于低速 Modem 中。

用数字数据的值调制载波的相位，这就是相移键控。例如用 180°相移表示“1”；用 0°相移表示“0”。这种调制方式抗干扰性能较好，而且相位的变化还可以作为定时信息来同步发送机和接收机的时钟。码元只取两个相位值的叫 2 相调制，码元取 4 个相位值的叫 4 相调制。

所谓 4 相相对相移键控（4DPSK）是利用前后两个码元之间的相对相位变化来表示二进制数据，其变化规律如下图所示，实线和虚线分别代表两种不同的调制方案，码元信号分布在复平面的同心圆上。这样可以用一个码元代表两位二进制数，能提供较高的数据速率，但实现技术更复杂。

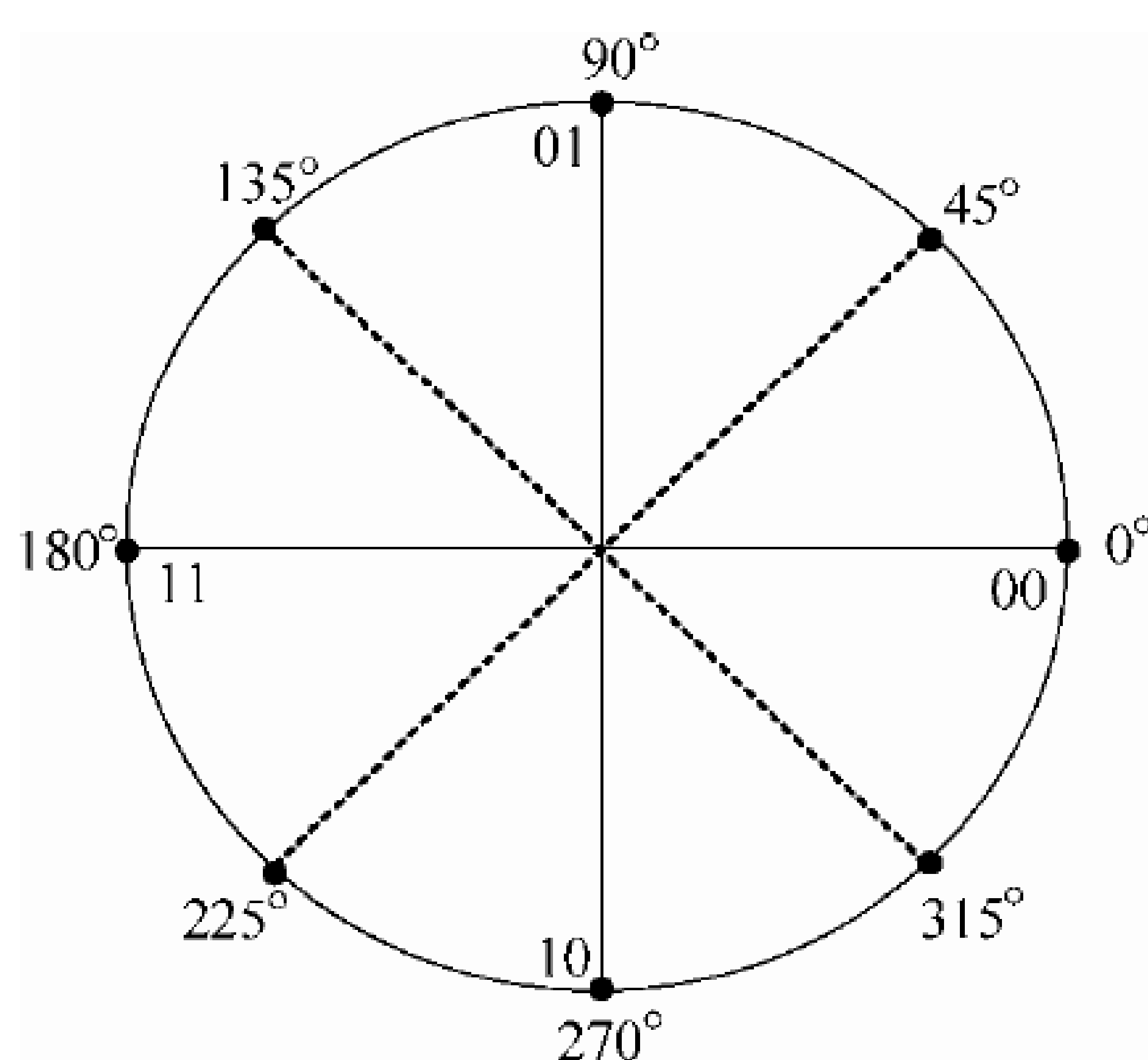


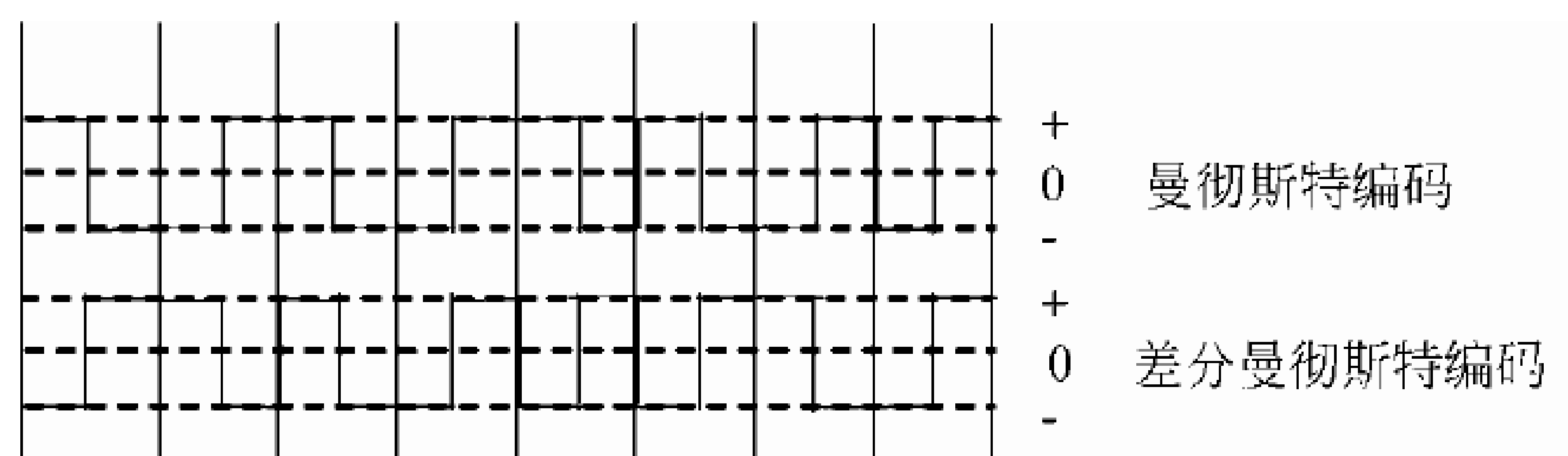

图　两种 4DPSK 调制方案

**参考答案**

（14）C

**试题（15）**

下图中画出了曼彻斯特编码和差分曼彻斯特编码的波形图，实际传送的比特串为＿（15）＿。




（15）A. 1　0　1　0　1　1　0　0

B. 0　1　1　1　0　0　1　0

C. 0　1　0　1　0　0　1　1

D. 1　0　0　0　1　1　0　1

**试题（15）分析**

曼彻斯特编码（Manchester Code）是一种双相码。可以用高电平到低电平的转换边表示“0”，而用低电平到高电平的转换边表示“1”，相反的表示也是允许的。比特中间的电平转换边既表示了数据代码，同时也作为定时信号使用。曼彻斯特编码使用在低速以太网中。

差分码又称相对码，在差分码中利用电平是否跳变来分别表示“1”或“0”，分为传号差分码和空号差分码。传号差分码是输入数据为“1”时，编码波型相对于前一代码电平产生跳变；输入为“0”时，波型不产生跳变。空号差分码是当输入数据为“0”时，编码波型相对于前一代码电平产生跳变；输入为“1”时，波型不产生跳变。

差分曼彻斯特编码兼有差分码和曼彻斯特编码的特点，与曼彻斯特编码不同的是，这种码元中间的电平转换边只作为定时信号，而不表示数据。差分曼彻斯特编码用在令牌环网中。

**参考答案**

（15）C

**试题（16）、（17）**

E1 信道的数据速率是<u>（16）</u>，其中每个话音信道的数据速率是<u>（17）</u>。

（16）A．1.544Mb/s　B．2.048Mb/s　C．6.312Mb/s　D．44.736Mb/s

（17）A．56kb/s　B．64kb/s　C．128kb/s　D．2048kb/s

**试题（16）、（17）分析**

时分多路复用（Time Division Multiplexing，TDM）要求各个子通道按时间片轮流地占用整个带宽。时间片的大小可以按一次传送一位、一个字节或一个固定大小的数据块所需的时间来确定。

时分多路复用按照子通道动态利用情况又可再分为两种：同步时分和统计时分。在同步时分制下，整个传输时间划分为固定大小的时槽，各子通道都占有一个固定位置的时槽。这样，在接收端可以按约定的时间关系恢复各子通道的信息流。当某个子通道的时槽来到时如果没有信息要传送，这一部分带宽就浪费了。

统计时分制是对同步时分制的改进。在发送端，集中器依次循环扫描各个子通道。若某个子通道有信息要发送则为它分配一个时槽，若没有信息就跳过，这样就没有空槽在线路上传播了。然而需要在每个时槽中加入一个控制字段，以便接收端可以确定该时槽是属于哪个子通道的。

在美国和日本使用的一种通信标准是贝尔系统的 T1 载波（见下图），它把 24 路话音信道按时分多路的原理复合在一条 1.544Mb/s 的高速信道上。该系统的工作是这样的，用一个编码解码器轮流对 24 路话音信道取样、量化和编码，一个取样周期（125μs）中得到的 7 位一组的数字合成一串，共 7×24 位长。这样的数字串在送入高速信道前要在每一个 7 位组的后面插入一个信令位，于是变成了 8×24=192 位长的数字串。这 192 位

数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125μs 传送一帧。每个子信道的数据速率为 56 kb/s。

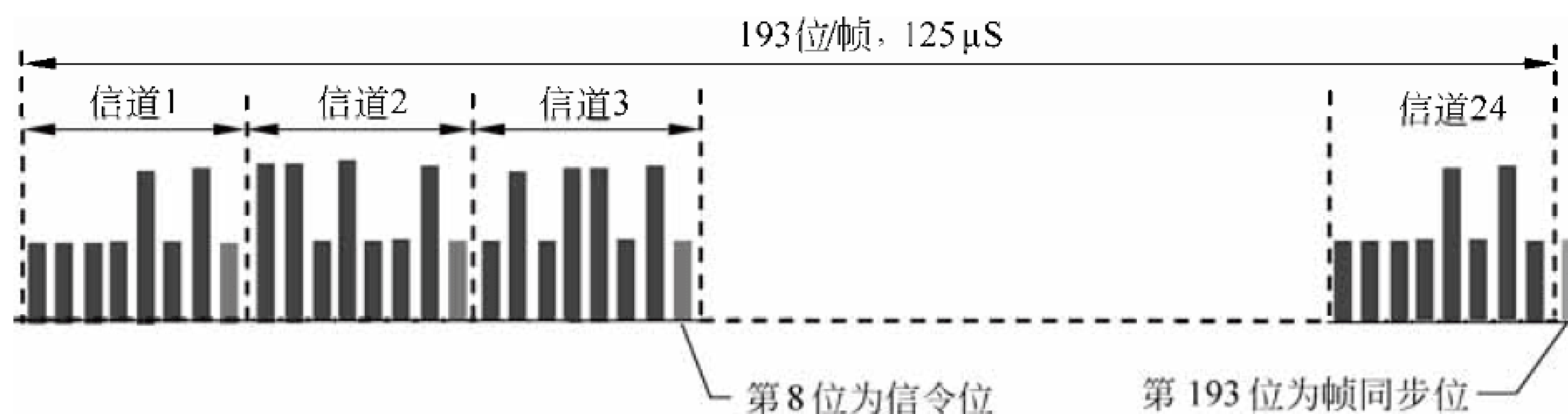



图　T1 载波

$T_1$ 载波还可以多路复用到更高级的载波上，4 个 1.544 Mb/s 的 $T_1$ 信道结合成 1 个 6.312Mb/s 的 $T_2$ 信道，7 个 $T_2$ 信道组合成 1 个 $T_3$ 信道，6 个 $T_3$ 信道组合成 1 个 $T_4$ 信道。

ITU-T 的 E1 信道的数据速率是 2.048 Mb/s（参见下图）。这种载波把 32 个 8 位一组的数据样本组装成125μs 的基本帧，其中 30 个子信道用于话音传送数据，2 个子信道（CH0 和 CH16）用于传送控制信令，每个子信道的数据速率为 64 kb/s。除了北美和日本外，E1 载波在其他地区得到广泛使用。

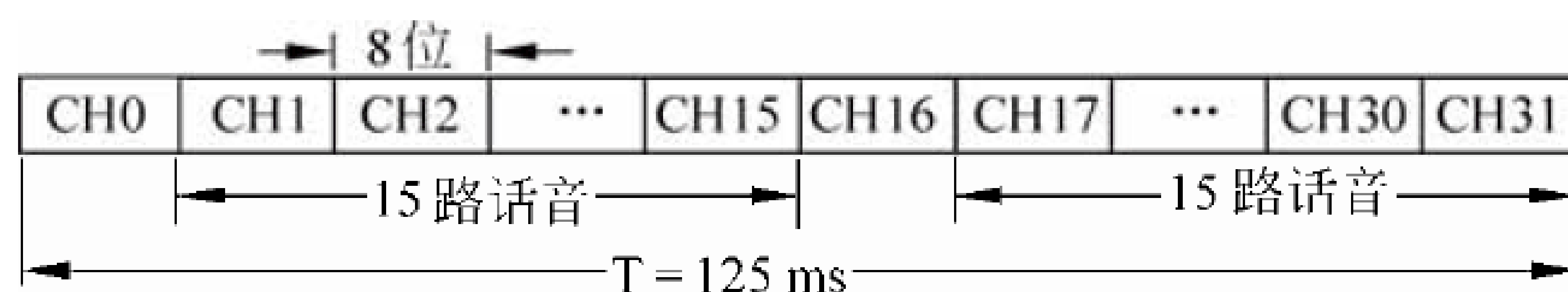



图　E1 帧

按照 ITU-T 的多路复用标准，E2 载波由 4 个 E1 载波组成，数据速率为 8.448Mb/s。E3 载波由 4 个 E2 载波组成，数据速率为 34.368 Mb/s。E4 载波由 4 个 E3 载波组成，数据速率为 139.264 Mb/s。E5 载波由 4 个 E4 载波组成，数据速率为 565.148 Mb/s。

**参考答案**

（16）B　（17）B

**试题（18）**

在各种 xDSL 技术中，能提供上下行信道非对称传输的是__（18）__。

（18）A．ADSL 和 HDSL　　B．ADSL 和 VDSL

C．SDSL 和 VDSL　　D．SDSL 和 HDSL

**试题（18）分析**

数字用户线（Digital Subscriber Line，DSL）是基于普通电话线的宽带接入技术，可以在一对铜质双绞线上同时传送数据和话音信号。DSL 有多种模式，统称为 xDSL。

根据上、下行传输速率是否相同，可以把 DSL 划分为对称和不对称两种传输模式。对称 DSL 的上、下行传输速率相同，用于代替传统的 T1/E1 接入线路。

对称数字用户线 SDSL（Symmetric Digital Subscriber Line）是一个通用的术语，涵盖了在一对或多对双绞线上提供不同数据速率的各种实现方式。SDSL 可以在一对双绞线上提供的对称速率范围为 128kb/s～2.32Mb/s，最常见的是 768kb/s，最大传输距离达 5km 以上。

高数据速率用户数字线（High-data-rate DSL，HDSL）采用两对双绞线提供全双工数据传输，支持 n×64kb/s（n=1，2，3，…）的各种速率，最高可达 1.544Mb/s 或 2.048Mb/s，传输距离可达 3～5km。HDSL 在视频会议、远程教学、移动电话基站连接等方面得到了广泛应用。HDSL2 是 HDSL 的演进版本，可以在一对双绞线上提供 1.5Mb/s 数据速率。

非对称 DSL 的上、下行传输速率不同，适用于对双向带宽要求不一样的应用，例如 Web 浏览、多媒体点播、信息发布等。

速率自适应用户数字线（Rate Adaptive DSL，RADSL）支持同步和非同步传输方式，下行速率为 640kb/s～12Mb/s，上行速率为 128kb/s～1Mb/s，也支持数据和语音同时传输。RADSL 具有速率自适应的特点，可以根据双绞线的质量和传输距离动态调整用户访问速率。RADSL 允许通信双方的 Modem 寻找流量最小的频道来传送数据，以保证一定的数据速率。RADSL 特别适用于线路质量千差万别的农村、山区等地区使用。

甚高比特率数字用户线（Very High Bit-rate DSL，VDSL）可在较短的距离上获得极高的传输速率，是各种 DSL 中速度最快的一种。在一对铜质双绞线上，VDSL 的下行速率可以扩展到 52Mb/s，同时支持 1.5～2.3Mb/s 的上行速率，但传输距离只有 300～1000m。当下行速率降至 13Mb/s 时，传送距离可达到 1.5km 以上，此时上行速率为 1.6～2.3Mb/s。传输距离的缩短，会使码间干扰大大减少，数字信号处理过程就大为简化，所以其设备成本要比 ADSL 低。

ADSL（Asymmetrical Digital Subscriber Line）是一种非对称 DSL 技术，在一对铜线上可提供上行速率 512kb/s～1Mb/s，下行速率 1～8Mb/s，有效传输距离在 3～5km。ADSL 在进行数据传输的同时还可以使用第三个信道提供 4kHz 的语音传输。现在比较成熟的 ADSL 标准有两种，即 G.DMT 和 G.Lite。

**参考答案**

（18）B

**试题（19）**

采用 ADSL 虚拟拨号接入方式中，用户端需要安装__（19）__软件。

（19）A．PPP　　　　B．PPPoE

C．PPTP　　　　D．L2TP

**试题（19）分析**

点对点协议 PPP（Point-to-Point Protocol）定义了一种封装机制，可以在点对点链路上传输多种协议的分组。PPP 应用在许多场合，例如家庭用户拨号上网，在 Modem 和网络中心之间要运行点对点协议；又例如局域网远程联网时要租用公网专线，可以通过

点对点协议来支持两个远程路由器之间的通信。

第 2 层隧道协议 L2TP（Layer 2 Tunneling Protocol）扩展了 PPP 模型，允许第二层连接端点和 PPP 会话端点驻留在由分组交换网连接的不同设备中。在 L2TP 模型中，用户通过第二层连接访问集中器，而集中器则把 PPP 帧通过隧道传送给网络访问服务器 NAS，从而把逻辑的 PPP 会话扩展到了帧中继或 Internet 这样的公共网络上。

PPTP（Point-to-Point Tunneling Protocol）是由 Microsoft、Ascend、3Com 和 ECI 等公司组成的 PPTP 论坛制定的第 2 层隧道协议。PPTP 定义了由接入集中器（PAC）和网络服务器（PNS）组成的客户机/服务器结构，用以支持虚拟专用网。

PPPoE（PPP over Ethernet）是把 PPP 协议封装在以太帧中传送，类似地，PPPoA（PPP over ATM）是把 PPP 协议封装在 ATM 虚电路中传送。ADSL 分为虚拟拨号和准专线两种接入方式。采用虚拟拨号方式的用户需要安装 PPPoE 或PPPoA客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门分配的静态或动态 IP 地址，开机即可接入 Internet。

**参考答案**

（19）B

**试题（20）、（21）**

ICMP 协议属于 TCP/IP 网络中的＿（20）＿协议，ICMP 报文封装在＿（21）＿包中传送。

（20）A．数据链路层　　B．网络层

C．传输层　　D．会话层

（21）A．IP　　B．TCP

C．UDP　　D．PPP

**试题（20）、（21）分析**

ICMP（Internet Control Message Protocol）与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠的提交。ICMP 报文有 11 种之多，报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

<table>
<tr><td>类型</td><td>代码</td><td>校验和</td></tr>
<tr><td colspan="3">参数</td></tr>
<tr><td colspan="3">信息（可变长）</td></tr>
</table>

图　ICMP 报文格式

**参考答案**

（20）B　（21）A

**试题（22）**

ARP 表用于缓存设备的 IP 地址与 MAC 地址的对应关系，采用 ARP 表的好处是__（22）__。

（22）A．便于测试网络连接数　　B．减少网络维护工作量
C．限制网络广播数量　　D．解决网络地址冲突

**试题（22）分析**

IP 地址是分配给主机的逻辑地址（或称协议地址），同时每个主机还有一个在子网内部唯一的 MAC 地址，我们把这个地址叫作物理地址或硬件地址。从网络互连的角度看，协议地址在整个互连网络中有效，而物理地址只是在子网内部有效；从网络协议分层的角度看，协议地址由网络层使用，而物理地址由数据链路层使用。

由于有两种地址，因而需要一种映像关系把这两种地址对应起来。在 Internet 中用地址分解协议（Address Resolution Protocol，ARP）来实现协议地址到物理地址的映像。ARP 分组的格式如下图所示。

| 硬件类型 | | 协议类型 |
|---|---|---|
| 硬件地址长度 | 协议地址长度 | 操作类型 |
| 发送结点硬件地址 | | |
| 发送结点协议地址 | | |
| 目标结点硬件地址 | | |
| 目标结点协议地址 | | |

图　ARP/RARP 分组格式

通常应用程序把要发送的报文交给 IP 协议，IP 当然知道接收方的协议地址（否则就不能通信了），但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路实体之前可以用两种方法得到目标结点的物理地址：

① 检查本地内存中的 ARP 地址映像表，其逻辑结构如下图所示。可以看出这是 IP 协议地址和以太网 MAC 地址的对照表。

② 如果在 ARP 表中查不到，就广播一个 ARP 请求分组，这种分组经过路由器进一步转发，可以到达所有连网的主机，其含义是：“如果你的 IP 地址是这个分组中的目标结点协议地址，请回答你的物理地址是什么”。收到该分组的主机一方面可以用分组中的两个源地址更新自己的 ARP 地址映像表；一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址，若不相符则不予回答。

可见，由于 ARP 表的存在，加速了 MAC 地址的查找，同时限制了网络中广播的 ARP 请求的数量。

| IP 地址 | 以太网地址 |
|---|---|
| 130.130.87.1 | 08 00 39 00 29 D4 |
| 129.129.52.3 | 08 00 5A 21 17 22 |
| 192.192.30.5 | 08 00 10 99 A1 44 |

图　ARP 地址映像表

**参考答案**

（22）C

**试题（23）**

以下有关边界网关协议 BGP4 的叙述中，不正确的是<u>（23）</u>。

（23）A．BGP4 网关向对等实体（Peer）发布可以到达的 AS 列表

B．BGP4 网关采用逐跳路由（hop-by-hop）模式发布路由信息

C．BGP4 可以通过路由汇聚功能形成超级网络（Supernet）

D．BGP4 报文直接封装在 IP 数据报中传送

**试题（23）分析**

边界网关协议（Border Gateway Protocol，BGP）是应用于自治系统（AS）之间的外部网关协议。BGP 基本上是一个距离矢量路由协议，但是与 RIP 协议采用的算法稍有区别。BGP 不但为每个目标计算最小通信费用，而且跟踪通向目标的路径；它不但把目标的通信费用发送给每一个邻居，而且也公告通向目标的最短路径（由 AS 的列表组成）。所以 BGP 采用的算法也叫作通路矢量路由（Path Vector Routing）算法。

BGP 算法没有距离矢量路由协议的不稳定性，可以避免路由循环。当 BGP 路由器收到一条路由信息时，首先检查它所在的自治系统是否在通路列表中。如果在列表中，则该路由信息被忽略，从而避免了出现路由循环。

BGP 支持无类别的域间路由（CIDR）。例如，某 ISP 有一个地址块，195.10.×.×，其中包含 256 个传统的 C 类网络，地址范围从 195.10.0.×到 195.10.255.×。BGP 协议可以把这 256 个 C 类网络组成一个超网（Supernet），与传统的 B 类网络一样大，并且向邻居发送一个有关地址块 195.10.×.×的公告，从而避免了发送 256 个 C 类网络的地址公告，同时也减小了路由表的大小。

BGP 邻居之间通过 TCP 连接交换路由信息，使用端口号 179。这意味着 BGP 不需要差错控制和流量控制。当检测到路由表改变时，BGP 只把改变了路由通过 TCP 连接发送给它的邻居。BGP 不需要周期地发送更新信息，BGP 路由更新公告通过最短的路径到达目标。

**参考答案**

（23）D

**试题（24）、（25）**

为了限制路由信息传播的范围，OSPF 协议把网络划分成 4 种区域（Area），其中 （24） 的作用是连接各个区域的传输网络， （25） 不接受本地自治系统之外的路由信息。

（24）A．不完全存根区域　　B．标准区域
　　　C．主干区域　　　　　D．存根区域

（25）A．不完全存根区域　　B．标准区域
　　　C．主干区域　　　　　D．存根区域

**试题（24）、（25）分析**

OSPF 定义了以下 5 种区域，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。

主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。

存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。

完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。

不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（24）C　（25）D

**试题（26）、（27）**

POP3 协议采用 （26） 模式，当客户机需要服务时，客户端软件（Outlook Express 或 FoxMail）与 POP3 服务器建立 （27） 连接。

（26）A．Browser/Server　　B．Client/Server
　　　C．Peer to Peer　　　D．Peer to Server

（27）A．TCP　　B．UDP
　　　C．PHP　　D．IP

**试题（26）、（27）分析**

POP3 协议采用 Client/Server 模式，当客户机需要服务时，客户端软件（Outlook Express 或 FoxMail）与 POP3 服务器建立 TCP 连接。

**参考答案**

（26）B　（27）A

**试题（28）**

SMTP 服务器端使用的端口号默认为＿（28）＿。

（28）A．21　　B．25　　C．53　　D．80

**试题（28）分析**

本题考查 TCP/IP 协议簇中几个重要的应用层协议相关知识。

TCP/IP 协议簇应用层几个常用协议及其服务端端口号如下表所示：

| 协议 | 使用的端口号 |
|---|---|
| HTTP | 80 |
| SMTP | 25 |
| POP | 110 |
| TELNET | 23 |
| FTP | 20、21 |

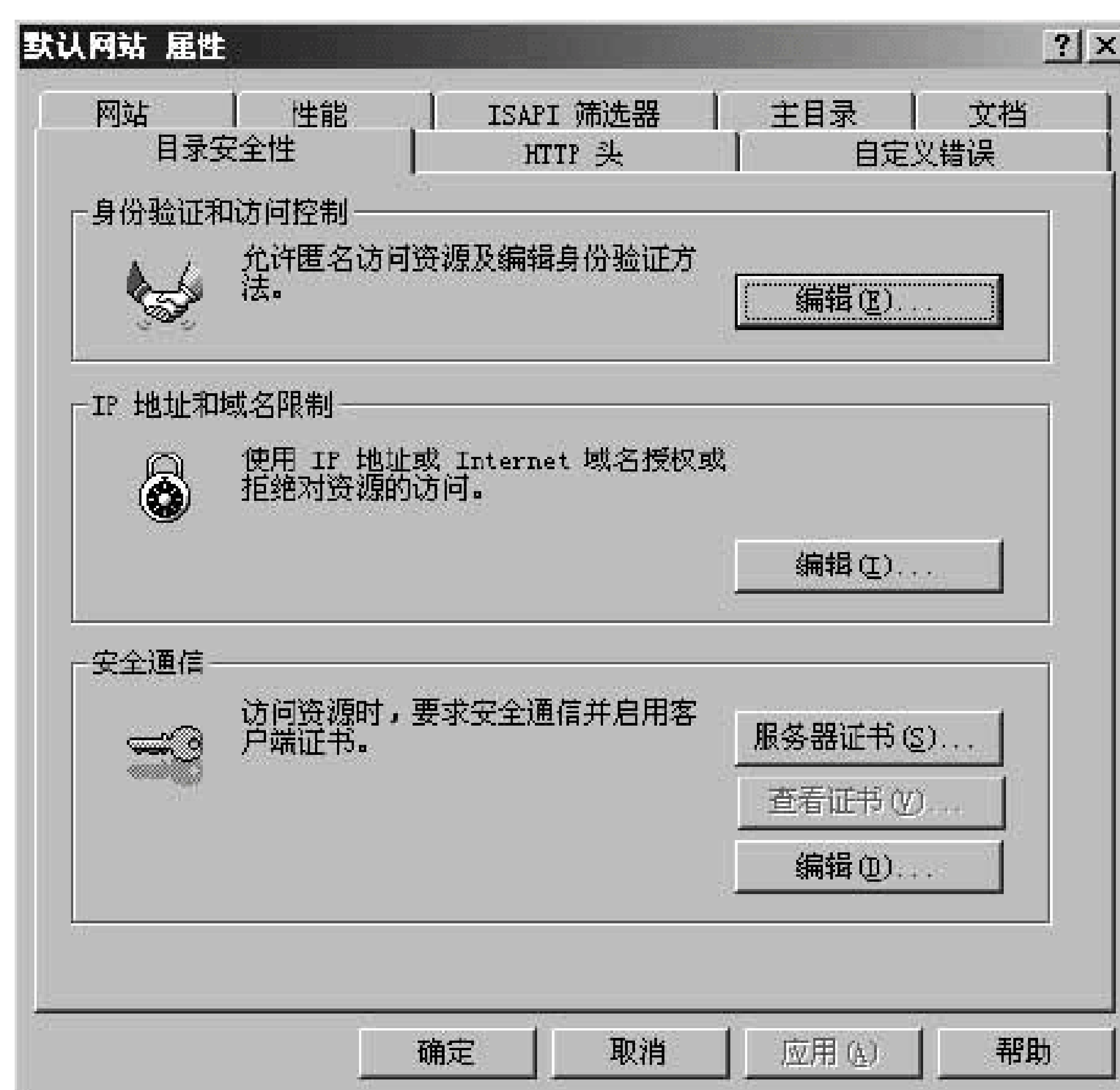
**参考答案**

（28）B

**试题（29）**

下图为 Web 站点的默认网站属性窗口，如果要设置用户对主页文件的读取权限，需要在＿（29）＿选项卡中进行配置。

（29）A．网站　　B．主目录　　C．文档　　D．HTTP 头




**试题（29）分析**

本题考查 Web 服务器配置相关知识。

在配置 Web 站点时，主目录选项卡中可配置主页文件的放置目录及用户对主页文件

的读取权限。

**参考答案**

（29）B

**试题（30）**

DHCP 客户端启动时会向网络发出一个 Dhcpdiscover 包来请求 IP 地址，其源 IP 地址为__（30）__。

（30）A．192.168.0.1　　B．0.0.0.0
　　C．255.255.255.0　　D．255.255.255.255

**试题（30）分析**

本题考查 DHCP 服务器配置相关知识。

DHCP 服务器配置完成后，客户端启动时会向网络发出一个 Dhcpdiscover 包来请求 IP 地址，由于此时尚未分配 IP 地址，故其源 IP 地址与目标 IP 地址均为 0.0.0.0。

**参考答案**

（30）B

**试题（31）**

当使用时间到达租约期的__（31）__时，DHCP 客户端和 DHCP 服务器将更新租约。

（31）A．50%　　B．75%　　C．87.5%　　D．100%

**试题（31）分析**

本题考查 DHCP 服务器配置相关知识。

当使用时间到达租约期的 50%时，DHCP 客户端和 DHCP 服务器将更新租约。

**参考答案**

（31）A

**试题（32）**

在 Linux 中，某文件的访问权限信息为“-rwxr--r--”，以下对该文件的说明中，正确的是__（32）__。

（32）A．文件所有者有读、写和执行权限，其他用户没有读、写和执行权限
　　B．文件所有者有读、写和执行权限，其他用户只有读权限
　　C．文件所有者和其他用户都有读、写和执行权限
　　D．文件所有者和其他用户都只有读和写权限

**试题（32）分析**

本题考查 Linux 基础知识。

在 Linux 操作系统中，为了保证文件信息的安全，Linux 给文件都设定了一定的访问权限。Linux 中的每一个文件都归某一个特定的用户所有，而且一个用户一般总是与某个用户组相关。Linux 对文件的访问设定了三级权限：文件所有者、与文件所有者同组的用户、其他用户。对文件的访问主要是三种处理操作：读取、写入和执行。三级访

问权限和三种处理操作的组合就形成了 9 种情况。可以用它来确定哪个用户可以通过何种方式对文件和目录进行访问和操作。同时，用户可以为自己的文件赋予适当的权限，以保证他人不能修改和访问。当用 ls -l 命令显示文件或目录的详细信息时，每一个文件或目录的列表信息分为四部分，其中最左边的一位是第一部分，标示 Linux 操作系统的文件类型，其余三部分是三组访问权限，每组用三位表示，如下图所示。

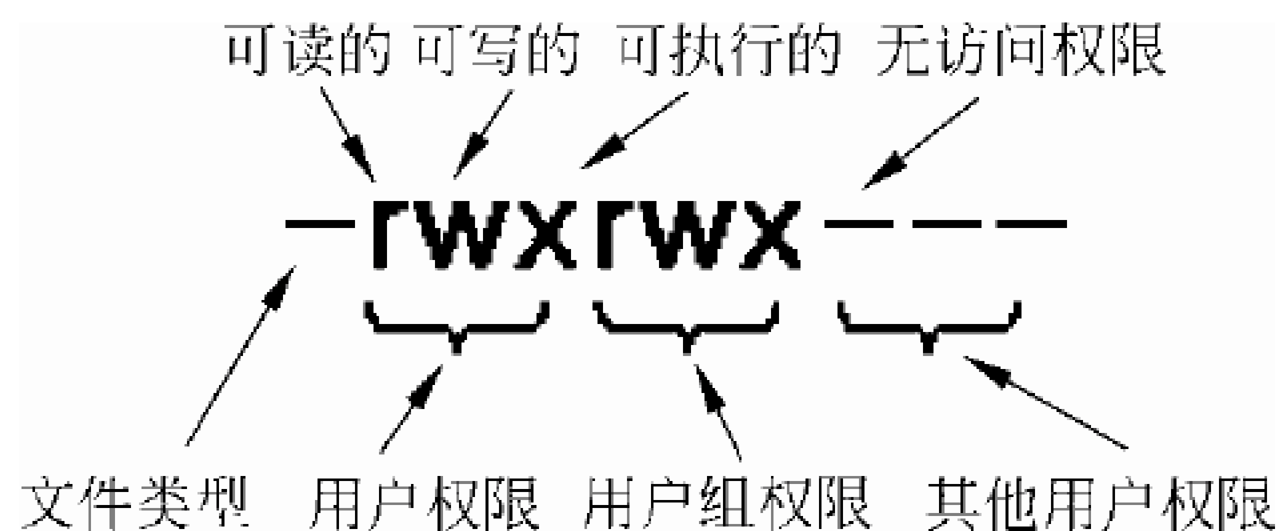



图　Linux 文件访问权限格式

**参考答案**

（32）B

**试题（33）**

在 Linux 中，更改用户口令的命令是__（33）__。

（33）A．pwd　　B．passwd　　C．kouling　　D．password

**试题（33）分析**

本题考查 Linux 基本命令。

pwd 是显示当前工作目录的命令，passwd 是更改用户口令的命令。

**参考答案**

（33）B

**试题（34）**

在 Linux 中，目录“/proc”主要用于存放__（34）__。

（34）A．设备文件　　B．命令文件　　C．配置文件　　D．进程和系统信息

**试题（34）分析**

本题考查 Linux 基础知识。

Linux 主要的系统目录及其简单描述如下：

- /bin：存放普通用户可以使用的命令文件。目录/usr/bin 也可用来存放用户命令。
- /sbin：一般存放非普通用户使用的命令（有时普通用户也可能会用到）。目录 /usr/sbin 中也包括了许多系统命令。
- /etc：系统的配置文件。
- /root：系统管理员（root 或超级用户）的主目录。
- /usr：包括与系统用户直接相关的文件和目录，一些主要的应用程序也保存在该目录下。

- /home：用户主目录的位置，保存了用户文件（用户自己的配置文件、文档、数据等）。
- /dev：设备文件所在目录。在 Linux 中设备以文件形式表现，从而可以按照操作文件的方式简便地对设备进行操作。
- /mnt：文件系统挂载点。一般用于安装移动介质，其他文件系统（如 DOS）的分区、网络共享文件系统或任何可安装的文件系统。
- /lib：包含许多由/bin 和/sbin 中的程序使用的共享库文件。目录/usr/lib/中含有更多用于用户程序的库文件。
- /boot：包括内核和其他系统启动时使用的文件。
- /var：包含一些经常改变的文件。例如假脱机（spool）目录、文件日志目录、锁文件、临时文件等。
- /proc：操作系统的内存映像文件系统，是一个虚拟的文件系统（没有占用磁盘空间）。查看时，看到的是内存里的信息，这些文件有助于了解系统内部信息。
- /initrd：在计算机启动时挂载 initrd.img 映像文件的目录以及载入所需设备模块的目录。
- /opt：存放可选择安装的文件和程序。主要由第三方开发者用于安装他们的软件包。
- /tmp：用户和程序的临时目录，该目录中的文件被系统定时自动清空。
- /lost+found：在系统修复过程中恢复的文件所在目录。

**参考答案**

（34）D

**试题（35）**

网络用户只能接收但不能发送 Email，其原因是__（35）__。

（35）A．邮件服务器配置错误

B．路由器端口的访问控制列表设置为 deny pop3

C．路由器端口的访问控制列表设置为 deny smtp

D．客户端代理设置错误

**试题（35）分析**

本题考查邮件服务器配置相关知识。

当邮件服务器配置错误时可能不能发送 Email；若路由器端口的访问控制列表设置为 deny pop3，会导致网络用户不能接收 Email，与能否发送 Email 无关；若路由器端口的访问控制列表设置为 deny smtp，会导致网络用户不能发送 Email；若客户端代理设置错误，比如发送服务器的域名设置错误，会导致网络用户不能发送 Email。

**参考答案**

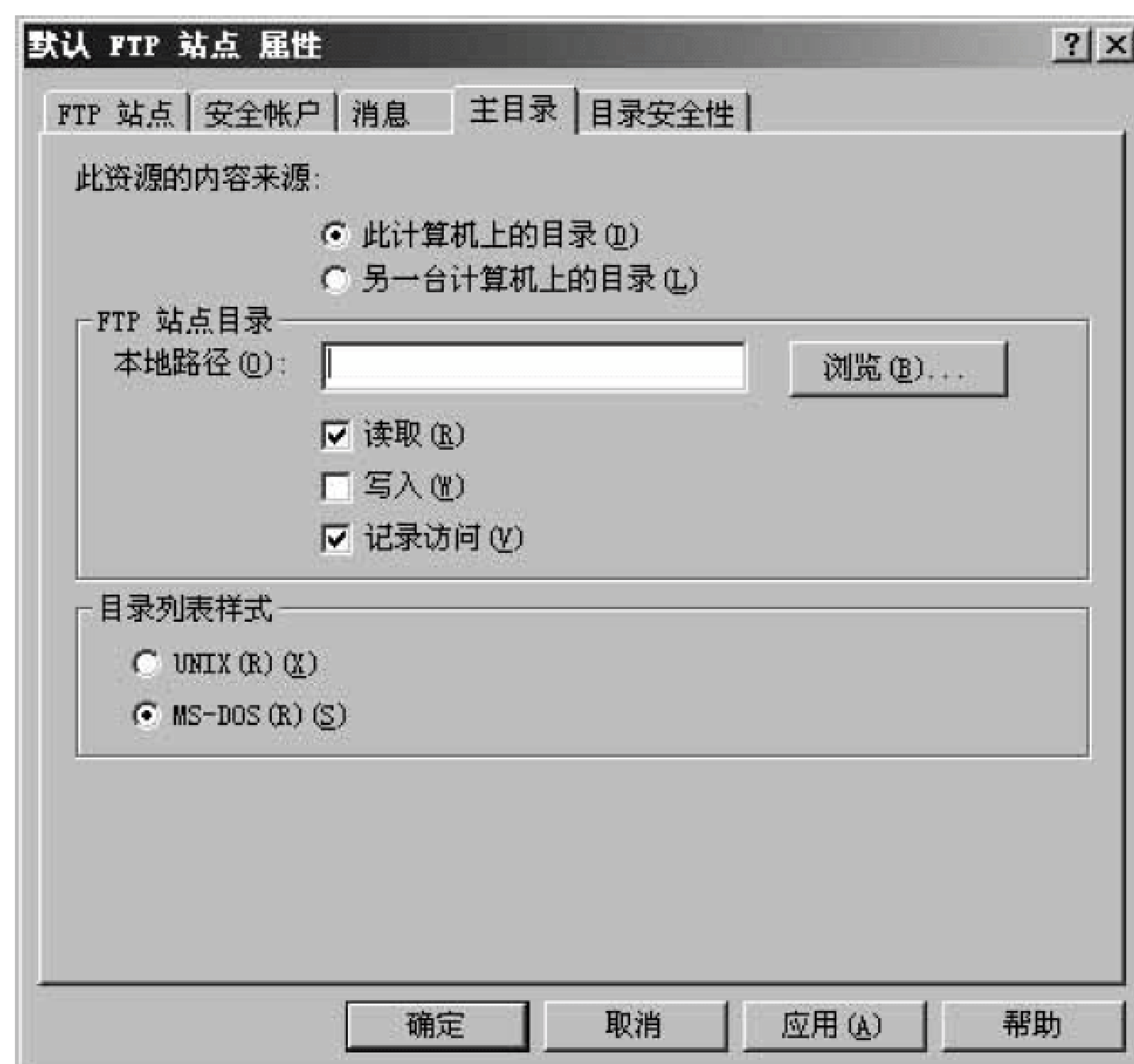
（35）B

**试题（36）**

配置 FTP 服务器的属性窗口如下图所示，默认情况下“本地路径”文本框中的值为__（36）__。

（36）A．c:\inetpub\wwwroot　　B．c:\inetpub\ftproot

C．c:\wmpubi\wwwroot　　D．c:\wmpubi\ftproot




**试题（36）分析**

本题考查 FTP 服务器配置相关知识。默认情况下，配置 FTP 服务器时“本地路径”文本框中的值为 c:\inetpub\ftproot。

**参考答案**

（36）B

**试题（37）、（38）**

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的__（37）__文件中寻找域名对应的 IP 地址。在该文件中，默认情况下必须存在的一条记录是__（38）__。

（37）A．hosts　　B．lmhosts　　C．networks　　D．dnsfile

（38）A.192.168.0.1　gateway　　B．224.0.0.0　multicast

C．0.0.0.0　source　　D．127.0.0.1　localhost

**试题（37）、（38）分析**

本题考查域名解析服务相关知识。

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的 hosts 文件中寻找域名对应的 IP 地址。hosts 文件有用户存放的域名与 IP 地址的对应关系，该文件中通常存在一条 127.0.0.1　localhost，用于设置本地环路。hosts 文件的内容如下图所示。

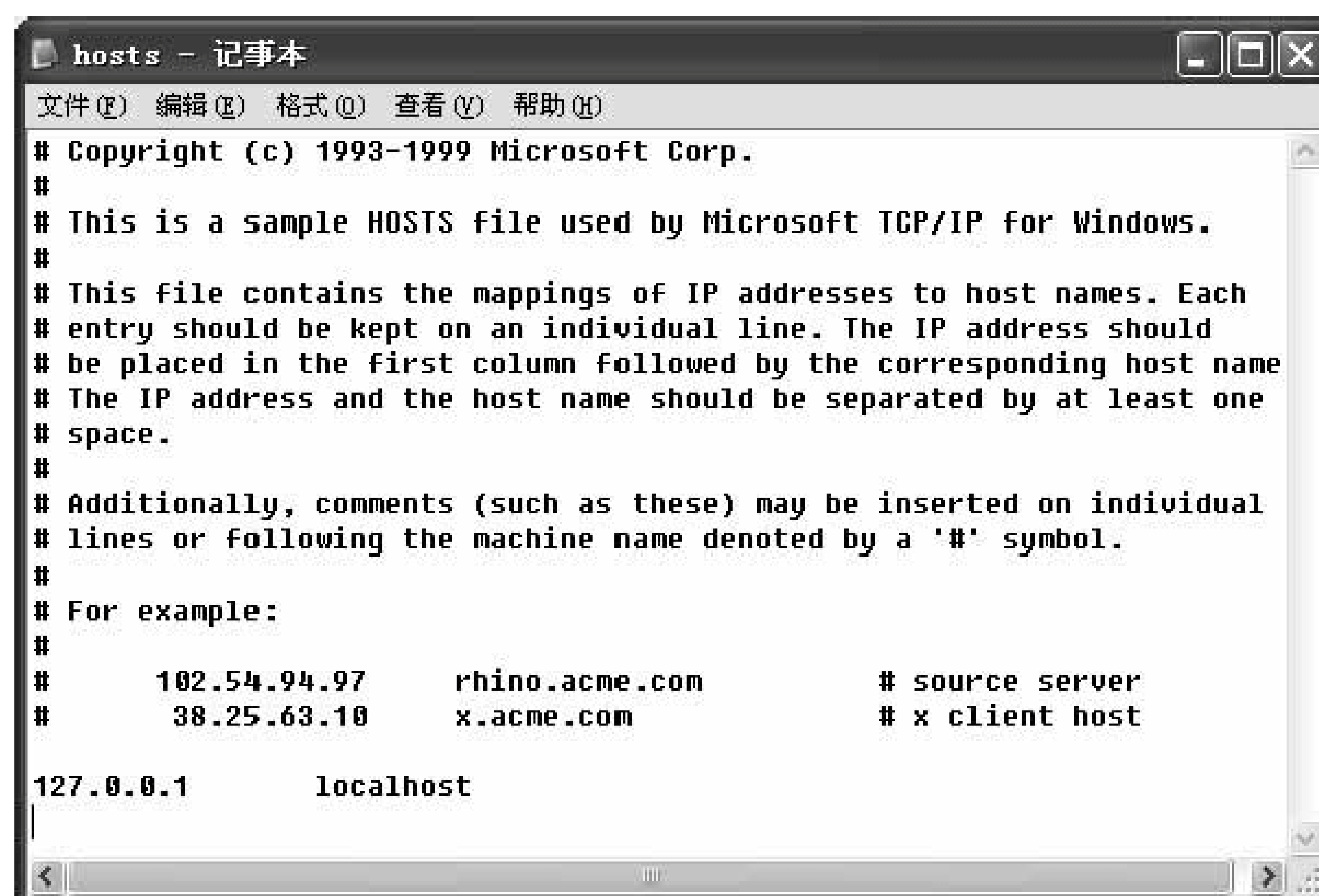


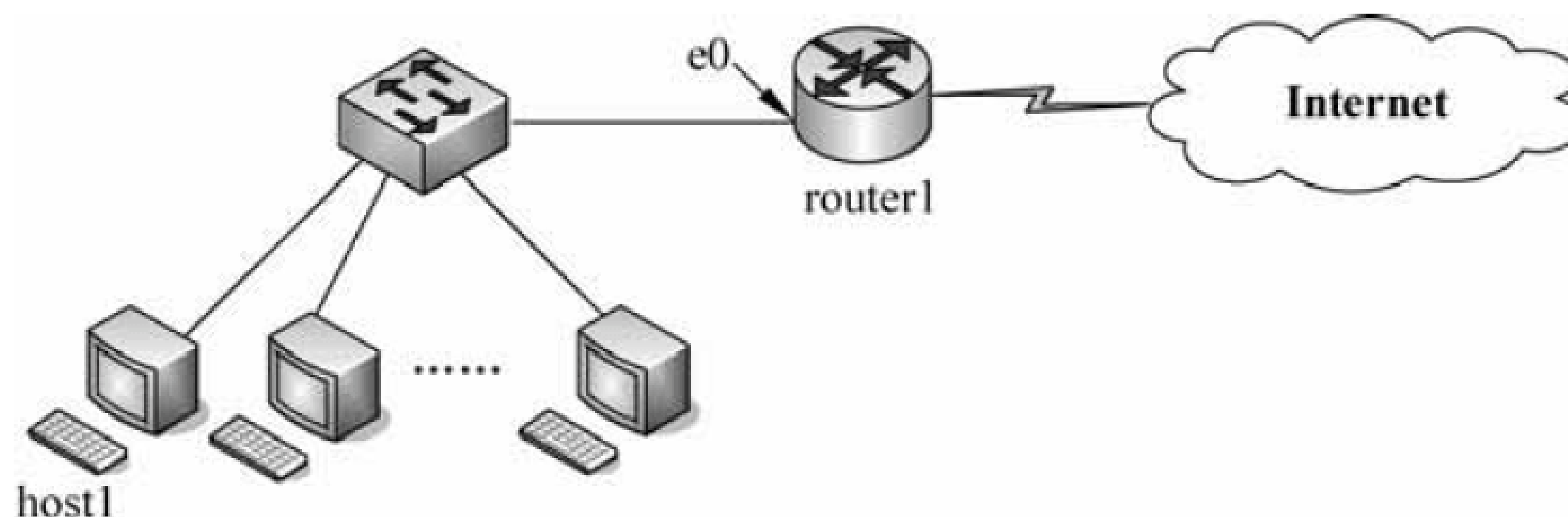

图　hosts 文件示例

## 参考答案

（37）A　（38）D

**试题（39）、（40）**

某网络拓扑结构如下图所示：




在主机 host1 的命令行窗口输入 tracert www.abc.com.cn 命令后，得到如下结果：

C:\Documents and Settings \User>tracert www.abc.com.cn

Tracing route to caelum.abc.com.cn [208.30.1.101]
over a maximum of 30 hops:

```
1    1 ms    1 ms   <1 ms    119.215.67.254
2    2 ms    1 ms    1 ms    172.116.11.2
3   71 ms    1 ms    1 ms    119.145.65.86
4    1 ms    1 ms    1 ms    172.116.141.6
5    1 ms    1 ms    1 ms    192.168.66.14
6    1 ms    1 ms   <1 ms    208.30.1.101
```

Trace complete.

则路由器 router1 e0 接口的 IP 地址为__（39）__；www.abc.com.cn 的 IP 地址为__（40）__。

（39）A．172.116.11.2　　B．119.215.67.254

C．210.120.1.30　　D．208.30.1.101

（40）A．172.116.11.2　　B．119.215.67.254

C．210.120.1.30　　D．208.30.1.101

**试题（39）、（40）分析**

本题考查网络配置及相关知识。

在输入 tracert 命令后记录的是到达目的主机所经过的所有路由的延迟时间及地址，故第一条记录应为本地网关地址，最后一条为目的主机地址，由此路由器 router1 e0 接口的 IP 地址为 119.215.67.254；www.abc.com.cn 的 IP 地址为 208.30.1.101。

**参考答案**

（39）B　（40）D

**试题（41）、（42）**

某报文的长度是 1000 字节，利用 MD5 计算出来的报文摘要长度是__（41）__位，利用 SHA 计算出来的报文摘要长度是__（42）__位。

（41）A．64　　B．128　　C．256　　D．160

（42）A．64　　B．128　　C．256　　D．160

**试题（41）、（42）分析**

本题考查网络安全方面关于报文摘要算法的基础知识。

报文摘要算法原理是用不定长的输入数据，通过散列方法转换成定长的输出，主要算法是 MD5 和 SHA，MD5 的输出长度是 128 位，SHA 的输出长度是 160 位，与报文本身的长度没有关系。

**参考答案**

（41）B　（42）D

**试题（43）**

以下安全协议中，用来实现安全电子邮件的协议是__（43）__。

（43）A．IPSec　　B．L2TP　　C．PGP　　D．PPTP

**试题（43）分析**

本题考查网络安全方面关于安全协议的基础知识。

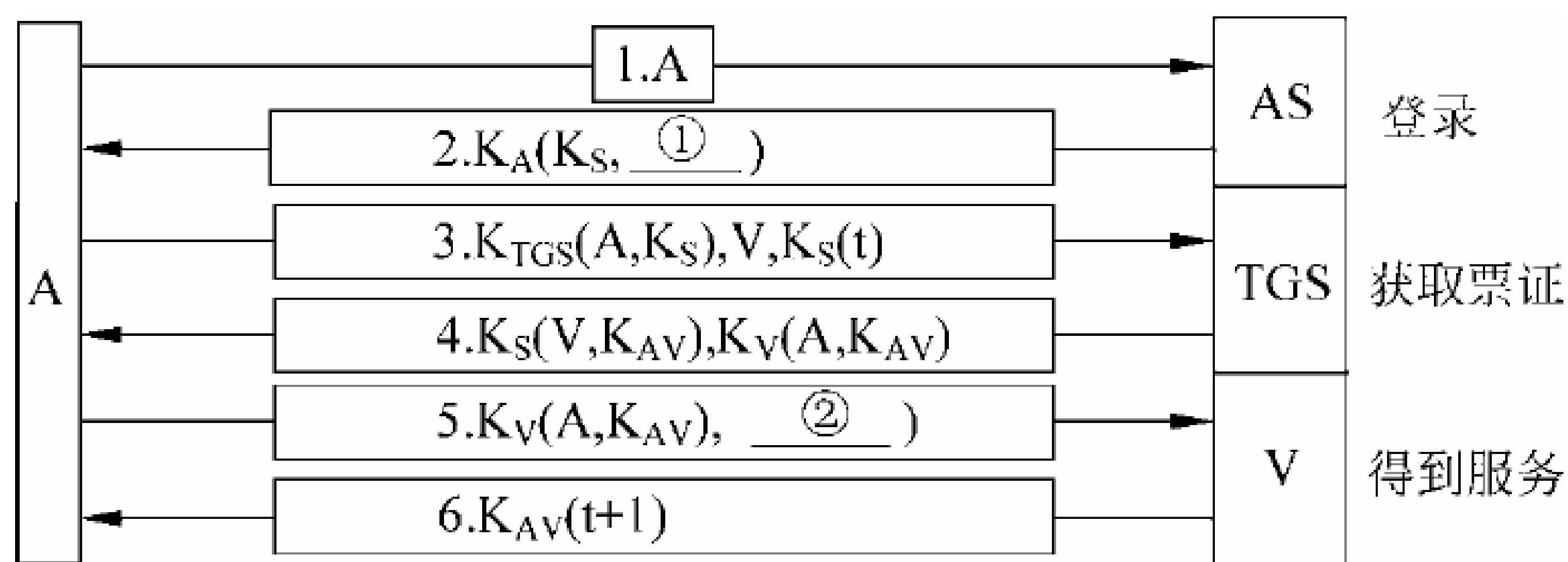
PGP（Pretty Good Privacy）是 Philip R．Zimmermann 在 1991 年开发的电子邮件加密软件包。PGP 已经成为使用最广泛的电子邮件加密软件。

**参考答案**

（43）C

**试题（44）、（45）**

Kerberos 由认证服务器（AS）和票证授予服务器（TGS）两部分组成，当用户 A 通过 Kerberos 向服务器 V 请求服务时，认证过程如下图所示，图中①处为__（44）__，②处为__（45）__。




（44）A. $K_{TGS}(A,K_S)$　B. $K_S(V,K_{AV})$　C. $K_V(A,K_{AV})$　D. $K_S(t)$

（45）A. $K_{AV}(t+1)$　B. $K_S(t+1)$　C. $K_S(t)$　D. $K_{AV}(t)$

**试题（44）、（45）分析**

本题考查网络安全方面关于安全协议的基础知识。

Kerberos由认证服务器（AS）和票证授予服务器（TGS）两部分组成，当用户A通过Kerberos向服务器V请求服务时，认证过程如下图所示：

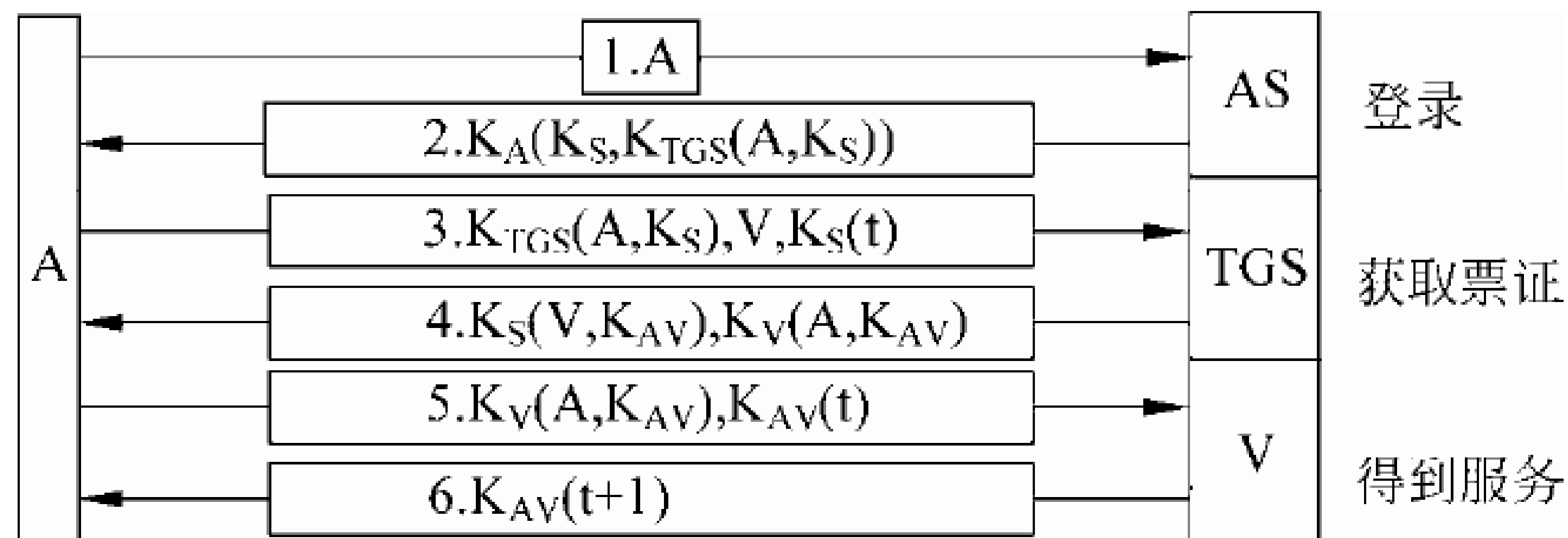



图　Kerberos认证过程

**参考答案**

（44）A　（45）D

**试题（46）**

公钥体系中，用户甲发送给用户乙的数据要用__（46）__进行加密。

（46）A. 甲的公钥　B. 甲的私钥　C. 乙的公钥　D. 乙的私钥

**试题（46）分析**

本题考查网络安全方面公钥体系的基础知识。

两个用户进行通信时，发送方可以用自身的私钥对数据进行签名，同时也可以用对方的公钥对数据进行加密，接收方收到数据后，用对方的公钥验证签名，用自身的私钥解密数据。

**参考答案**

（46）C

**试题（47）**

RMON和SNMP的主要区别是__（47）__。

（47）A. RMON只能提供单个设备的管理信息，而SNMP可以提供整个子网的管

理信息

B．RMON 提供了整个子网的管理信息，而 SNMP 管理信息库只包含本地设备的管理信息

C．RMON 定义了远程网络的管理信息库，而 SNMP 只能提供本地网络的管理信息

D．RMON 只能提供本地网络的管理信息，而 SNMP 定义了远程网络的管理信息库

**试题（47）分析**

SNMP 是应用层协议，它通过 UDP 数据报实现管理站与远程代理之间的通信，如下图所示。每个被管理设备中的代理实现管理信息库 MIB-2，只能收集本地的管理信息。所以最初定义的 SNMP 协议只能提供单个设备的网络管理信息，例如进出某个远程设备的分组数或字节数等。

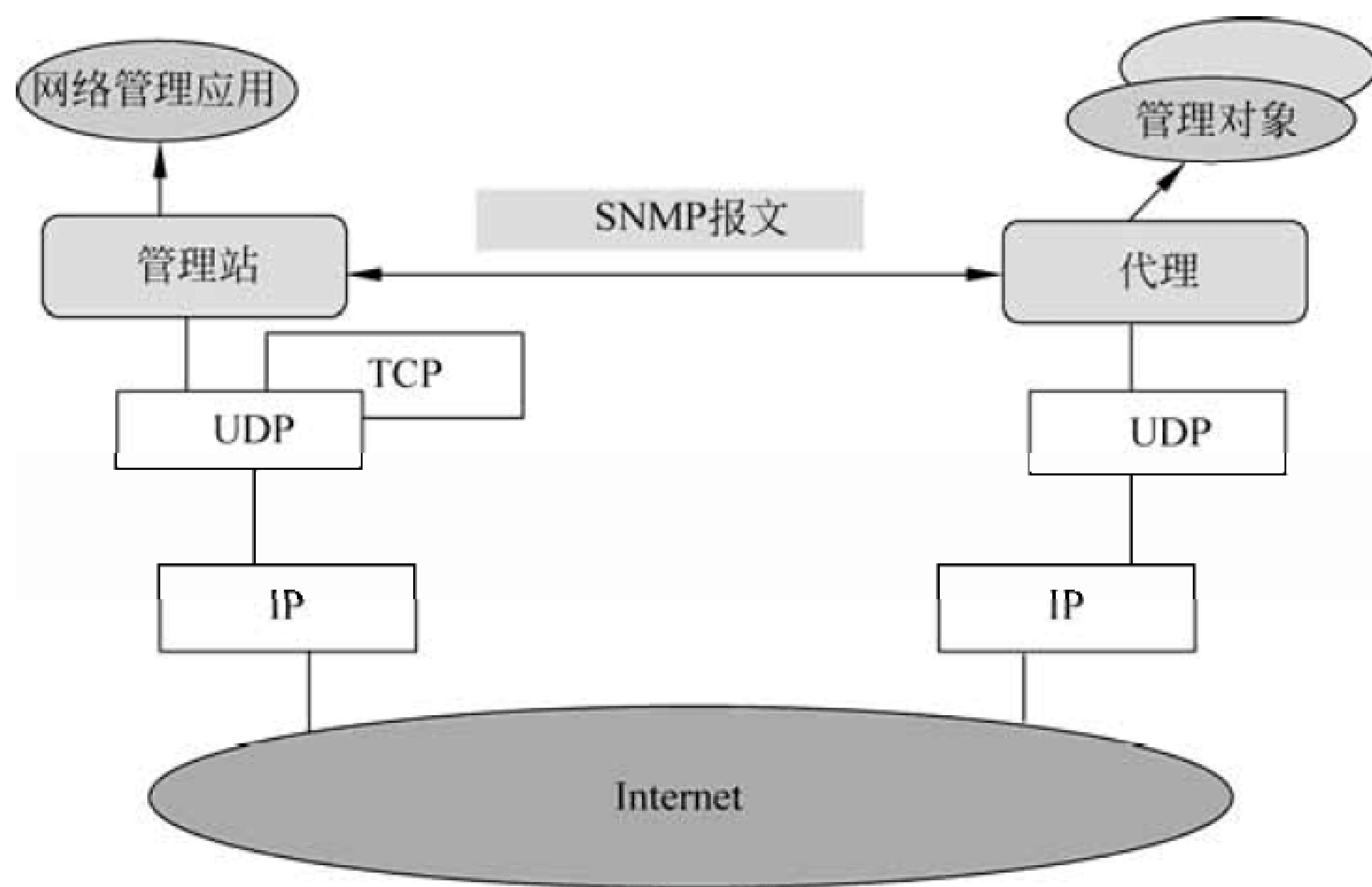



图　简单网络管理协议的体系结构

用于监视整个网络通信情况的设备叫作网络监视器（Monitor）或探测器（Probe），这种设备观察 LAN 上出现的每个分组，并进行统计和汇总，例如提供出错统计数据（残缺分组数、冲突次数）、性能统计数据（每秒钟提交的分组数、分组大小的分布情况）等，如下图所示。RMON 探测器（RMON Probe）实现 RMON 管理信息库（RMON MIB），并且响应管理站的查询请求。所以 RMON 可以提供整个子网的管理信息。

**参考答案**

（47）B

**试题（48）**

SNMP 采用 UDP 提供的数据报服务传递信息，这是由于＿（48）＿。

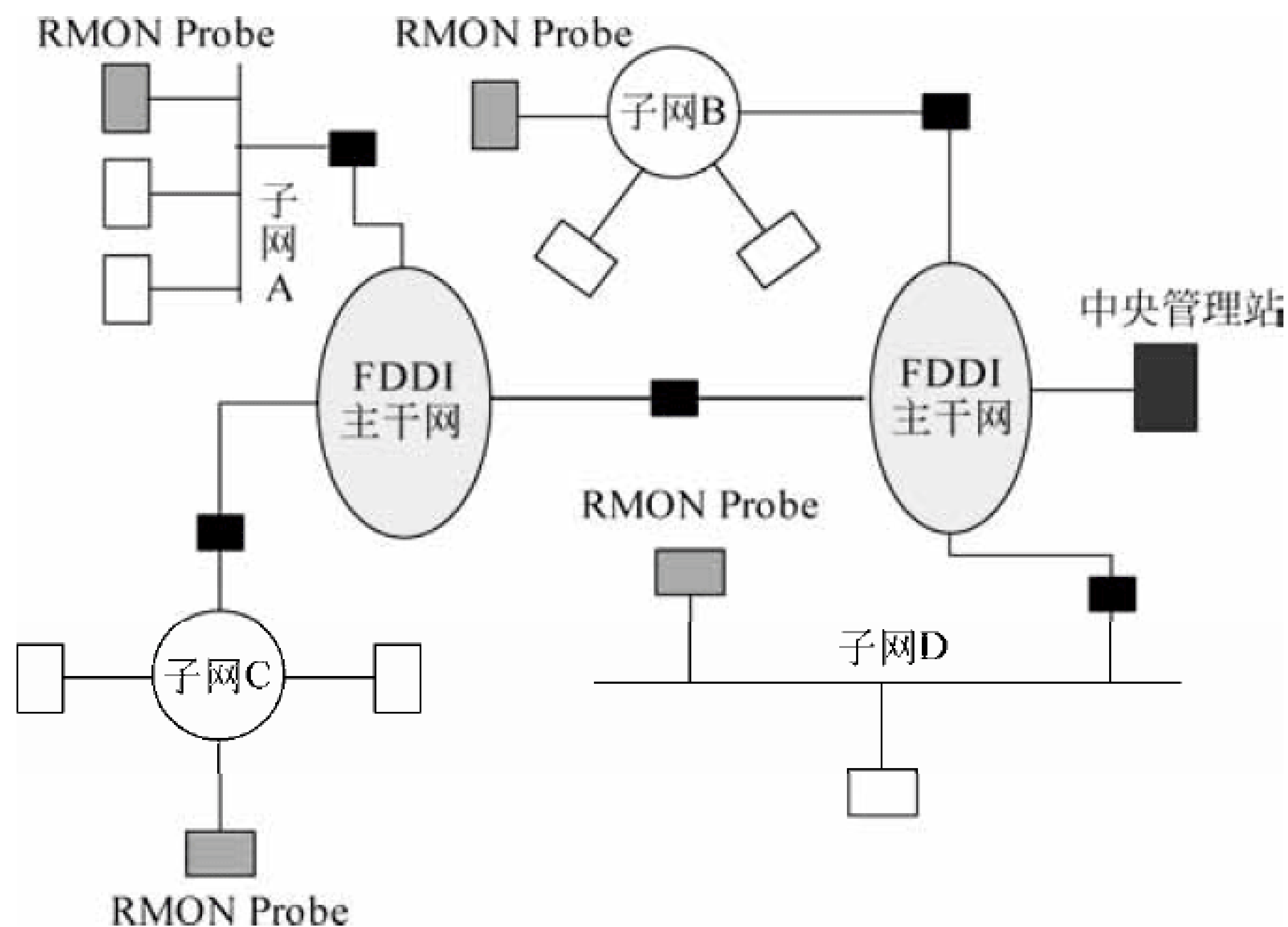



图　远程网络监视的配置

（48）A．UDP 比 TCP 更加可靠
　　B．UDP 数据报文可以比 TCP 数据报文大
　　C．UDP 是面向连接的传输方式
　　D．UDP 实现网络管理的效率较高

**试题（48）分析**

SNMP 是应用层协议，采用 UDP 数据报服务传送网络管理报文。其所以选择 UDP 协议而不是 TCP 协议，这是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不是很可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现的建议是对每个管理信息要装配成单独的数据报独立发送，而且报文应短些，不要超过 484 个字节。

**参考答案**

（48）D

**试题（49）**

在网络管理中要防止各种安全威胁。在 SNMP 中，无法预防的安全威胁是__（49）__。

（49）A．篡改管理信息：通过改变传输中的 SNMP 报文实施未经授权的管理操作
　　B．通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息
　　C．假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作
　　D．消息泄露：SNMP 引擎之间交换的信息被第三者偷听

**试题（49）分析**

SNMPv3 把对网络协议的安全威胁分为主要的和次要的两类。标准规定安全模块必须提供防护的两种主要威胁是：

① 修改信息（Modification of Information）：就是某些未经授权的实体改变了进来的

SNMP 报文，企图实施未经授权的管理操作，或者提供虚假的管理对象。

② 假冒（Masquerade）：即未经授权的用户冒充授权用户的标识，企图实施管理操作。

SNMPv3 标准还规定安全模块必须对两种次要威胁提供防护：

① 修改报文流（Message Stream Modification）：由于 SNMP 协议通常是基于无连接的传输服务，重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。

② 消息泄露（Disclosure）：SNMP 引擎之间交换的信息可能被偷听，对这种威胁的防护应采取局部的策略。

有两种威胁是安全体系结构不必防护的，因为它们不是很重要，或者这种防护没有多大作用：

① 拒绝服务（Denial of Service）：因为在很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全子系统不必采取措施。

② 通信分析（Traffic Analysis）：即由第三者分析管理实体之间的通信规律，从而获取需要的信息。由于通常都是由少数管理站来管理整个网络，所以管理系统的通信模式是可预见的，防护通信分析就没有多大作用了。

**参考答案**

（49）B

**试题（50）**

在 Windows 的 DOS 窗口中键入命令

C:\> nslookup

> set type=ptr

> 211.151.91.165

这个命令序列的作用是＿（50）＿。

（50）A．查询 211.151.91.165 的邮件服务器信息

B．查询 211.151.91.165 到域名的映射

C．查询 211.151.91.165 的资源记录类型

D．显示 211.151.91.165 中各种可用的信息资源记录

**试题（50）分析**

nslookup 命令用于显示 DNS 查询信息，诊断和排除 DNS 故障。nslookup 有交互式和非交互式两种工作方式。

所谓非交互式工作就是只使用一次 nslookup 命令后又返回到 cmd.exe 提示符下。如果只查询一项信息，可以进入这种工作方式。nslookup 命令后面可以跟随一个或多个命令行选项，用于设置查询参数。每个命令行选项由一个连字符“-”后跟选项的名字组成，有时还要加一个等号“=”和一个数值。

如果需要查找多项数据，可以使用 nslookup 的交互工作方式。在 cmd.exe 提示符下键入 nslookup 后回车，就进入了交互工作方式，命令提示符变成“>”。

```
> set type=ptr                                                   #查询PTR记录
> 211.151.91.165                                                 #由地址查域名
服务器:  [61.134.1.4]
Address:  61.134.1.4

非权威应答:
165.91.151.211.in-addr.arpa     name = 165.tsinghua.edu.cn       #查询成功，得到域名
> www.tsinghua.edu.cn                                            #由域名查地址
服务器:  [61.134.1.4]
Address:  61.134.1.4

DNS request timed out.
    timeout was 2 seconds.
非权威应答:
www.tsinghua.edu.cn     canonical name = www.d.tsinghua.edu.cn

d.tsinghua.edu.cn
        primary name server = dns.d.tsinghua.edu.cn              #没有查出地址
        responsible mail addr = szhu.dns.edu.cn                   但给出了SOA记录
        serial  = 2007042815
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

图　查询 ptr 记录

在交互方式下，可以用 set type 命令设置查询的资源记录类型。DNS 服务器中主要的资源记录有 A（域名到 IP 地址的映射）、PTR（IP 地址到域名的映射）、MX（邮件服务器及其优先级）、CNAM（别名）和 NS（区域的授权服务器）等类型。通过 A 记录可以由域名查地址，也可以由地址查域名。当查询 PTR 记录时，可以由地址查到域名，参见上图。

**参考答案**

（50）B

**试题（51）、（52）**

32 位的 IP 地址可以划分为网络号和主机号两部分。下面的地址中__（51）__不能作为目标地址，__（52）__不能作为源地址。

（51）A．0.0.0.0　　B．127.0.0.1　　C．10.0.0.1　　D．192.168.0.255/24

（52）A．0.0.0.0　　B．127.0.0.1　　C．10.0.0.1　　D．192.168.0.255/24

**试题（51）、（52）分析**

网络号为 0 是指本地网络，主机号为 0 是指本地主机，所以 0.0.0.0 不能作为目标地址。主机号为全 1 的是广播地址，而地址 192.168.0.255/24 是一个 C 类广播地址，所以

不能作为源地址。

**参考答案**

（51）A　（52）D

**试题（53）～（55）**

假设用户 Q1 有 2000 台主机，则必须给他分配＿（53）＿个 C 类网络，如果分配给用户 Q1 的超网号为 200.9.64.0，则指定给 Q1 的地址掩码为＿（54）＿；假设给另一用户 Q2 分配的 C 类网络号为 200.9.16.0～200.9.31.0，如果路由器收到一个目标地址为 11001000 00001001 01000011 00100001 的数据报，则该数据报应送给用户＿（55）＿。

（53）A．4　　B．8　　C．10　　D．16

（54）A．255.255.255.0　　B．255.255.250.0

　　C．255.255.248.0　　D．255.255.240.0

（55）A．Q1　　B．Q2　　C．Q1 或 Q2　　D．不可到达

**试题（53）～（55）分析**

每一个 C 类网络可以分配的主机地址数为 254 个，所以对 Q1 用户必须分配给 8 个 C 类网络，其地址掩码应该为 255.255.248.0。路由器查找路由表时把目标地址与每个表项进行对比，

目标地址为　　11001000 00001001 01000011 00100001

Q1 的地址 200.9.64.0　　11001000 00001001 01000000 00000000/22

Q2 的地址 200.9.16.0　　11001000 00001001 00010000 00000000/20

按照最长匹配规则，显然目标地址与 Q1 的地址匹配。

**参考答案**

（53）B　（54）C　（55）A

**试题（56）**

建筑物综合布线系统中工作区子系统是指＿（56）＿。

（56）A．由终端到信息插座之间的连线系统

　　B．楼层接线间的配线架和线缆系统

　　C．各楼层设备之间的互连系统

　　D．连接各个建筑物的通信系统

**试题（56）分析**

结构化布线系统分为六个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统。

工作区子系统是指由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器，以及传感器等多种终端设备。

信息插座的类型应根据终端设备的种类而定。信息插座的安装分为嵌入式（新建筑

物）和表面安装（老建筑物）两种方式，信息插座通常安装在工作间四周的墙壁下方，距离地面 30cm，也有的安装在用户办公桌上。通常一个信息插座需要 9 平方米的空间。

**参考答案**

（56）A

**试题（57）**

设有下面 4 条路由：196.34.129.0/24、196.34.130.0/24、196.34.132.0/24 和 196.34.133.0/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是__（57）__。

（57）A．196.34.128.0/21　　B．196.34.128.0/22

C．196.34.130.0/22　　D．196.34.132.0/23

**试题（57）分析**

196.34.129.0/24 的二进制表示是 **11000100 00100010 10000001** 00000000

196.34.130.0/24 的二进制表示是 **11000100 00100010 10000010** 00000000

196.34.132.0/24 的二进制表示是 **11000100 00100010 10000100** 00000000

196.34.133.0/24 的二进制表示是 **11000100 00100010 10000101** 00000000

从中可以看出，经过路由会聚的地址应该是 196.34.128.0/21。

**参考答案**

（57）A

**试题（58）**

IPv6 地址 33AB:0000:0000:CD30:0000:0000:0000:0000/60 可以表示成各种简写形式，以下写法中，正确的是__（58）__。

（58）A．33AB:0:0:CD30::/60　　B．33AB:0:0:CD3/60

C．33AB::CD30/60　　D．33AB::CD3/60

**试题（58）分析**

IPv6 地址扩展到 128 位。$2^{128}$ 足够大，这个地址空间可能永远用不完。事实上，这个数足够为地球上每个分子分配一个 IP 地址。

IPv6 地址采用冒号分隔的十六进制数表示，例如下面是一个 IPv6 地址

8000:0000:0000:0000:0123:4567:89AB:CDEF

为了便于书写，规定了一些简化写法。首先，每个字段前面的 0 可以省去，例如 0123 可以简写为 123；其次一个或多个全 0 字段 0000 可以用一对冒号代替。例如以上地址可简写为

8000::123:4567:89AB:CDEF

因此，答案 B 的错误在于 CD30 不能省略成 CD3，答案 C 的错误在于::之间 0 的个数无法确定，答案 D 的错误综合了 B 和 C 的错误。

**参考答案**

（58）A

**试题（59）、（60）**

配置路由器时，PC 的串行口与路由器的__（59）__口相连，路由器与 PC 串行口通信的默认数据速率为__（60）__。

（59）A．以太接口　　B．串行接口　　C．RJ-45 端口　　D．console 接口

（60）A．2400b/s　　B．4800b/s　　C．9600b/s　　D．10Mb/s

**试题（59）、（60）分析**

第一次配置路由器必须通过控制台端口来访问，这也是最常用、最有效的配置方法。控制台端口是路由器的基本端口，连接控制台端口的线缆称为控制台电缆（Console Cable）。控制台电缆一端插入路由器的控制台端口，另一端插入 PC 的串行口，参见下图。




图　通过控制台端口访问路由器

计算机与路由器连接好以后，进入系统桌面，执行“开始”→“所有程序”→“附件”→“通讯”→“超级终端”命令，然后配置连接的默认参数。路由器与 PC 串行口通信的默认数据速率为 9600b/s，参见下图。




图　连接属性

**参考答案**

（59）D　（60）C

**试题（61）**

交换机命令 SwitchA(VLAN) #vtp pruning 的作用是__（61）__。

（61）A. 退出 VLAN 配置模式　　B. 删除一个 VLAN
　　C. 进入配置子模式　　D. 启动路由修剪功能

**试题（61）分析**

VLAN 中继协议（VLAN Trunking Protocol，VTP）用于简化 VLAN 的管理。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为服务器模式（Server）、客户机模式（Client）和透明模式（Transparent）。只有在服务器模式下，交换机才能创建和修改 VLAN 配置。在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛（flood）到所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

例如，在下图中，PC-A、PC-B、PC-E 和 PC-F 同属于 VLAN 1（用粗虚线表示）。如果 PC-A 产生了一个广播包，则交换机 A 将把它转发给连接 PC-B 的接入链路，也转发到连接交换机 B 的中继链路，因为中继链路是任何 VLAN 的成员。这种转发是有意义的，因为 PC-E 和 PC-F 连接在交换机 B 上，而它们与 PC-A 同属于 VLAN 1。

在下图中，PC-C 和 PC-D 是 VLAN 2（用细虚线表示）的成员。如果 PC-C 产生了一个本地广播包，显然交换机 A 会将其发送给 PC-D 的接入端口，然而若交换机 A 将这个广播包通过中继链路洪泛到交换机 B 则是无意义的，因为那里没有属于 VLAN 2 的设备。

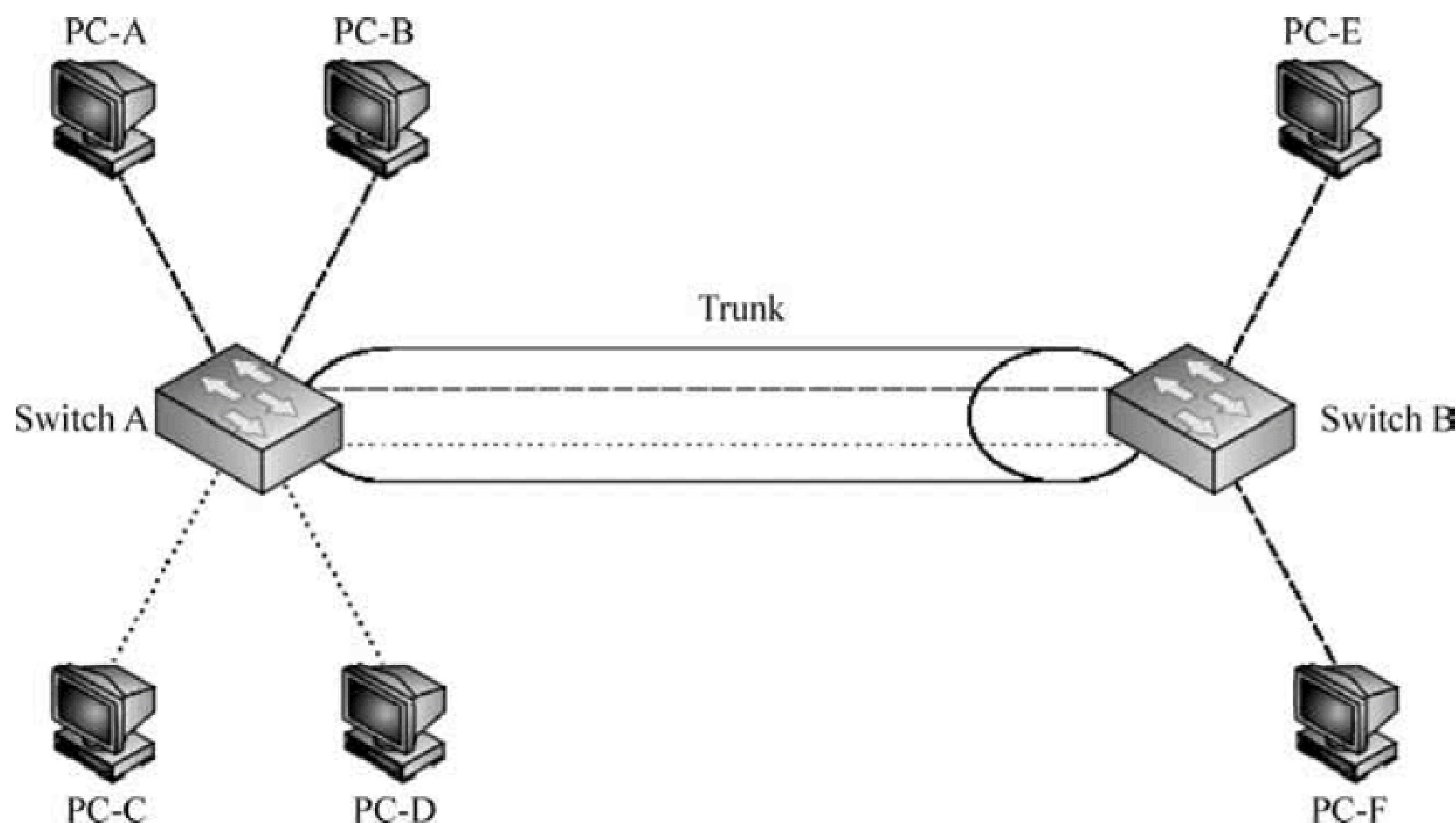



图　VLAN 之间的洪泛发送

为了解决这个问题，可以使用静态或动态的修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN，在下图中，两个交换机之间的一条中继链路已经被剪掉了。

但是，手工修剪会遇到一些问题，如果后来在交换机 B 上添加了 VLAN 2 的成员，则必须重新改变两个交换机的配置，并在中继链路上添加 VLAN 2 的中继连接。在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错。在这种情况下，并不是每一个 VLAN 都在每一个交换机上处于活动状态，并且很可能会在某条中继链路上剪掉不应该修剪的 VLAN，从而出现连接问题。

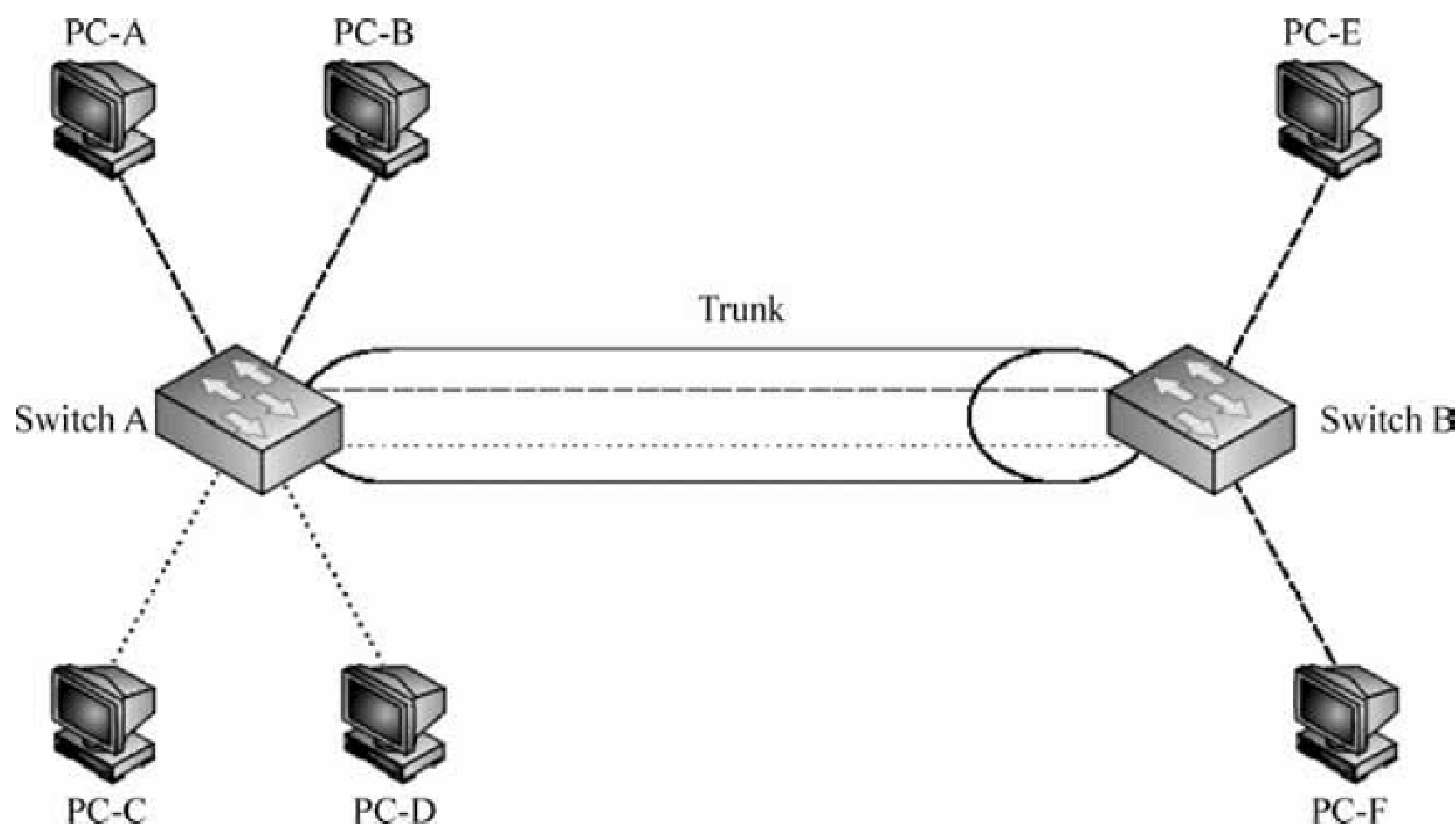



图　经过手工修剪的中继链路

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 可以告诉交换机 B，它有两个活动的 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

VTP 动态修剪的缺点是它要求在 VTP 域中的所有交换机都必须配置成服务器。由于交换机在服务器模式下工作时可以改变 VLAN 配置，也可以接受 VLAN 配置的改变，所以当多个管理员在多个服务器上同时配置 VLAN 时将会出现难以预见的后果。

**参考答案**

（61）D

**试题（62）、（63）**

以太网介质访问控制策略可以采用不同的监听算法，其中一种是：“一旦介质空闲就发送数据，假如介质忙，继续监听，直到介质空闲后立即发送数据”，这种算法称为__（62）__监听算法。这种算法的主要特点是__（63）__。

（62）A. 1-坚持型　　　　　　　　B. 非坚持型
　　　C. P-坚持型　　　　　　　　D. 0-坚持型

（63）A. 介质利用率低，且冲突概率低
　　　B. 介质利用率高，但冲突概率也高
　　　C. 介质利用率低，且无法避免冲突
　　　D. 介质利用率高，且可以有效避免冲突

**试题（62）、（63）分析**

在以太网上采用 CSMA 协议，其基本原理是，站在发送数据之前，先监听信道上是否有别的站发送的载波信号。若有，说明信道正忙；否则信道是空闲的。然后根据预定的策略决定，是立即发送，还是继续监听。

监听算法有三种：

第一种是非坚持型监听算法，其处理思路是：当一个站准备好帧，发送之前先监听信道，若信道空闲，立即发送，若信道忙，则后退一个随机时间，再监听信道并重复上述过程。由于随机时延后退，从而减少了冲突的概率；然而，可能因后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

第二种是 1-坚持型监听算法，其处理思路是：当一个站准备好帧，发送之前先监听信道，若信道空闲，立即发送，否则继续监听，直到信道空闲后立即发送。这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

第三种是 P-坚持型监听算法，其处理思路是：

① 若信道空闲，以概率 P 发送，以概率（1−P）延迟一个时间单位τ（网络传输时延）。

② 若信道忙，继续监听直到信道空闲，转①。

③ 如果发送延迟一个时间单位τ，则重复①。

这种算法汲取了以上两种算法的优点，但较为复杂。

**参考答案**

（62）A　（63）B

**试题（64）**

采用 CSMA/CD 协议的基带总线，其段长为 1000m，中间没有中继器，数据速率为 10Mb/s，信号传播速度为 200m/μs，为了保证在发送期间能够检测到冲突，则该网络上的最小帧长应为<u>（64）</u>比特。

（64）A. 50　　　B. 100　　　C.150　　　D. 200

**试题（64）分析**

带冲突检测的监听算法把浪费带宽的时间减少到检测冲突的时间。对局域网来说这个时间是很短的。通过分析确定，在基带系统中检测冲突需要的最长时间为 2τ，即网络传播延迟时间的两倍。

与冲突窗口相关的参数是最小帧长。如果在 2τ时间内帧已经发送完毕，这样发送站在整个发送期间将检测不到冲突。为了避免这种情况，网络标准中根据设计的数据速率和最大网段长度规定了最小帧长 $L_{min}$：

$$L_{min} = 2R \times d / v$$

这里 $R$ 是网络数据速率，$d$ 为最大段长，$v$ 是信号传播速度。有了最小帧长的限制，发送站必须对较短的帧增加填充位，使其等于最小帧长。接收站对收到的帧要检查长度，小于最小帧长的帧被认为是冲突碎片而丢弃。

根据题中给出的条件，可以计算如下：

$$L_{min} = 2R \times d / v = 2 \times 10\text{Mb/s} \times 1000\text{m} / 200\text{m/}\mu\text{s} = 100\text{bit}$$

**参考答案**

（64）B

**试题（65）**

以下属于万兆以太网物理层标准的是＿（65）＿。

（65）A．IEEE 802.3u　　B．IEEE 802.3a
　　C．IEEE 802.3e　　D．IEEE 802.3ae

**试题（65）分析**

2002 年 6 月，IEEE 发布了万兆以太网标准 802.3ae，其规定的几种传输介质如下表所示。传统以太网采用 CSMA/CD 协议，而万兆以太网基本应用于点到点线路，不再共享带宽，也没有冲突检测，所以，载波监听和多路访问技术不再重要。千兆以太网和万兆以太网采用与传统以太网同样的帧结构。

<table>
<tr><th>名　　称</th><th>电　　缆</th><th>最大段长</th><th>特　　点</th></tr>
<tr><td rowspan="2">10GBase-S(Short)</td><td>50μm 的多模光纤</td><td>300m</td><td rowspan="2">850nm 串行</td></tr>
<tr><td>62.5μm 的多模光纤</td><td>65m</td></tr>
<tr><td>10GBase-L(Long)</td><td>单模光纤</td><td>10km</td><td>1310nm 串行</td></tr>
<tr><td>10GBase-E(Extended)</td><td>单模光纤</td><td>40km</td><td>1550nm 串行</td></tr>
<tr><td rowspan="3">10GBase-LX4</td><td>单模光纤</td><td>10km</td><td rowspan="3">1310nm<br>4×2.5Gb/s<br>波分多路复用（WDM）</td></tr>
<tr><td>50μm 的多模光纤</td><td>300m</td></tr>
<tr><td>62.5μm 的多模光纤</td><td>300m</td></tr>
</table>

**参考答案**

（65）D

**试题（66）**

IEEE 802.11 采用了类似于 802.3 CSMA/CD 协议的 CSMA/CA 协议，之所以不采用 CSMA/CD 协议的原因是＿（66）＿。

（66）A．CSMA/CA 协议的效率更高　　B．为了解决隐蔽终端问题

C．CSMA/CD 协议的开销更大　　D．为了引进其他业务

**试题（66）分析**

CSMA/CA 叫作载波监听多路访问/冲突避免协议，与 CSMA/CD 协议的区别是不再使用冲突检测技术。在无线网中进行冲突检测是困难的。例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔（Inter Frame Spacing，IFS）时间。另外还有一个后退计数器，它的初始值是随机设置的，递减计数直到 0。基本的操作过程是：

① 如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

② 听到信道空闲后等待 IFS 时间，然后开始计数。最先计数完的站可以开始发送。

其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成开始发送。

分析这个算法发现，两次 IFS 之间的间隔是各个站竞争发送到时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

**参考答案**

（66）B

**试题（67）**

无线局域网（WLAN）标准 IEEE 802.11g 规定的最大数据速率是＿（67）＿。

（67）A．1Mb/s　　B．11Mb/s　　C．5Mb/s　　D．54Mb/s

**试题（67）分析**

IEEE 802.11 标准的制定始于 1987 年。1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM（Industrial Scientific and Medical）频段，采用扩频通信技术，支持 1Mb/s 和 2Mb/s 数据速率。随后又出现了两个新的标准，1998 年推出的 IEEE 802.11b 标准也是运行在 ISM 频段，采用 CCK（Complementary Code Keying）技术，支持 11Mb/s 的数据速率。1999 年推出的 IEEE 802.11a 标准运行在 U-NII（Unlicensed National Information Infrastructure）频段，采用 OFDM 调制技术，支持最高达 54Mb/s 的数据速率。2003 年推出的 IEEE 802.11g 标准运行在 ISM 频段，与 IEEE 802.11b 兼容，数据速率提高到 54Mb/s。下表列出了目前广泛使用的 4 种 WLAN 标准。

| 名　称 | 发布时间 | 工 作 频 段 | 调 制 技 术 | 数 据 速 率 |
|---|---|---|---|---|
| 802.11 | 1997 年 | 2.4GHz ISM 频段 | DB/SK<br>DQPSK | 1Mb/s<br>2Mb/s |
| 802.11b | 1998 年 | 2.4GHz ISM 频段 | CCK | 5.5Mb/s，11Mb/s |
| 802.11a | 1999 年 | 5GHz U-NII 频段 | OFDM | 54Mb/s |
| 802.11g | 2003 年 | 2.4GHz ISM 频段 | OFDM | 54Mb/s |

**参考答案**

（67）D

**试题（68）**

大型局域网通常组织成分层结构（核心层、汇聚层和接入层），以下关于网络核心层的叙述中，正确的是＿（68）＿。

（68）A．为了保障安全性，应该对分组进行尽可能多的处理

B．将数据分组从一个区域高速地转发到另一个区域

C．由多台二、三层交换机组成

D．提供用户的访问控制

**试题（68）分析**

大型园区网是一种具有复杂互连结构的局域网，通常被划分成不同的功能层次，典型的层次结构如下图所示。这种层次结构有利发挥联网设备的最大效率，使得故障定位可分级进行，便于维护和管理，也便于网络拓扑的后续扩展。

在三层模型中，核心层提供不同区域之间的高速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

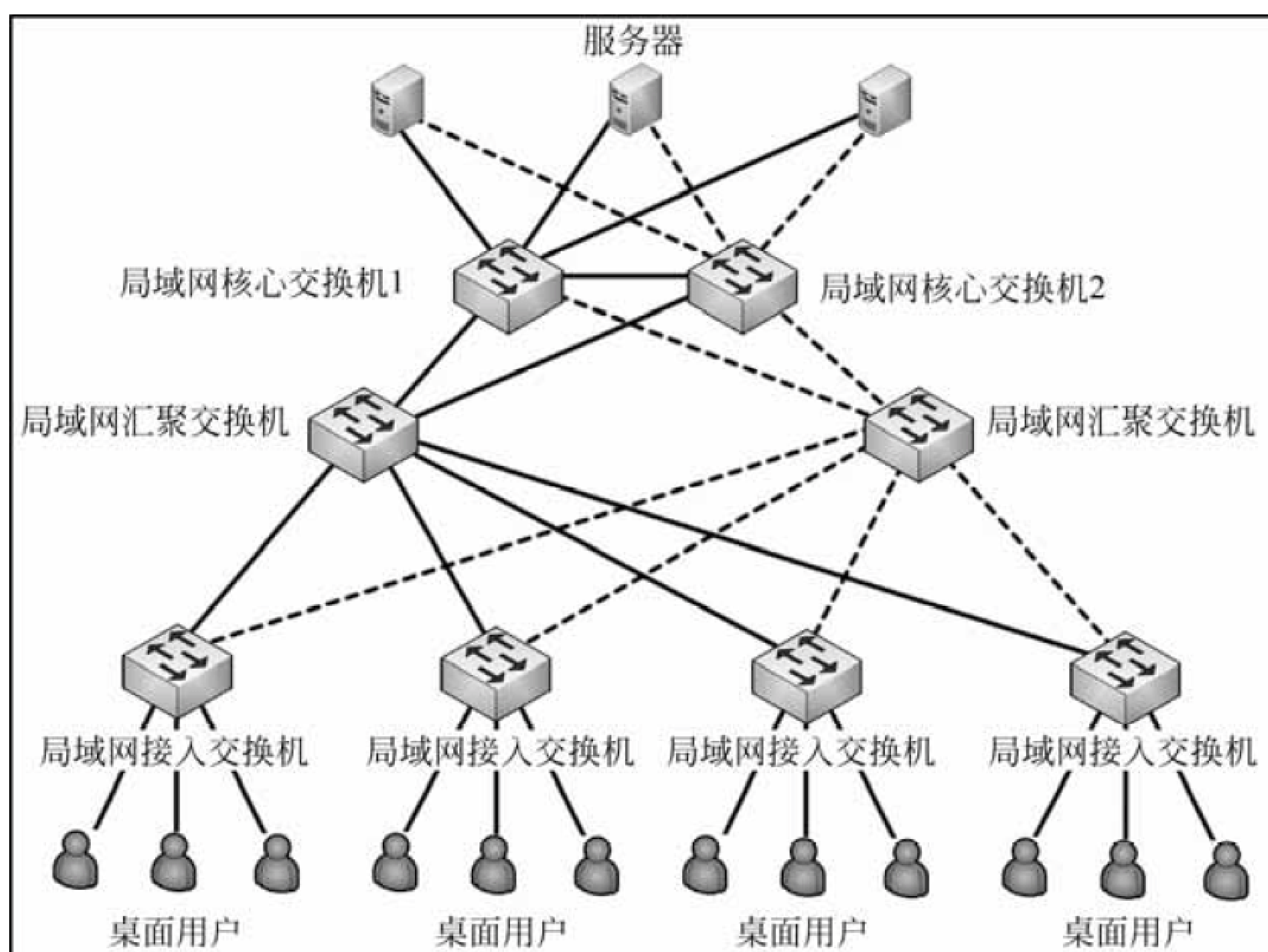



图　分层次的局域网结构

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。在设计核心层设备的功能时应避免使用数据包过滤、策略

路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的可管理性。核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。

汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问；接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等；接入层要负责收集用户信息（例如用户 IP 地址、MAC 地址、访问日志等），作为计费和排错的依据，

**参考答案**

（68）B

**试题（69）、（70）**

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，各个阶段都要产生相应的文档，以下选项中，<u>（69）</u>应该属于逻辑网络设计文档，<u>（70）</u>属于物理网络设计文档。

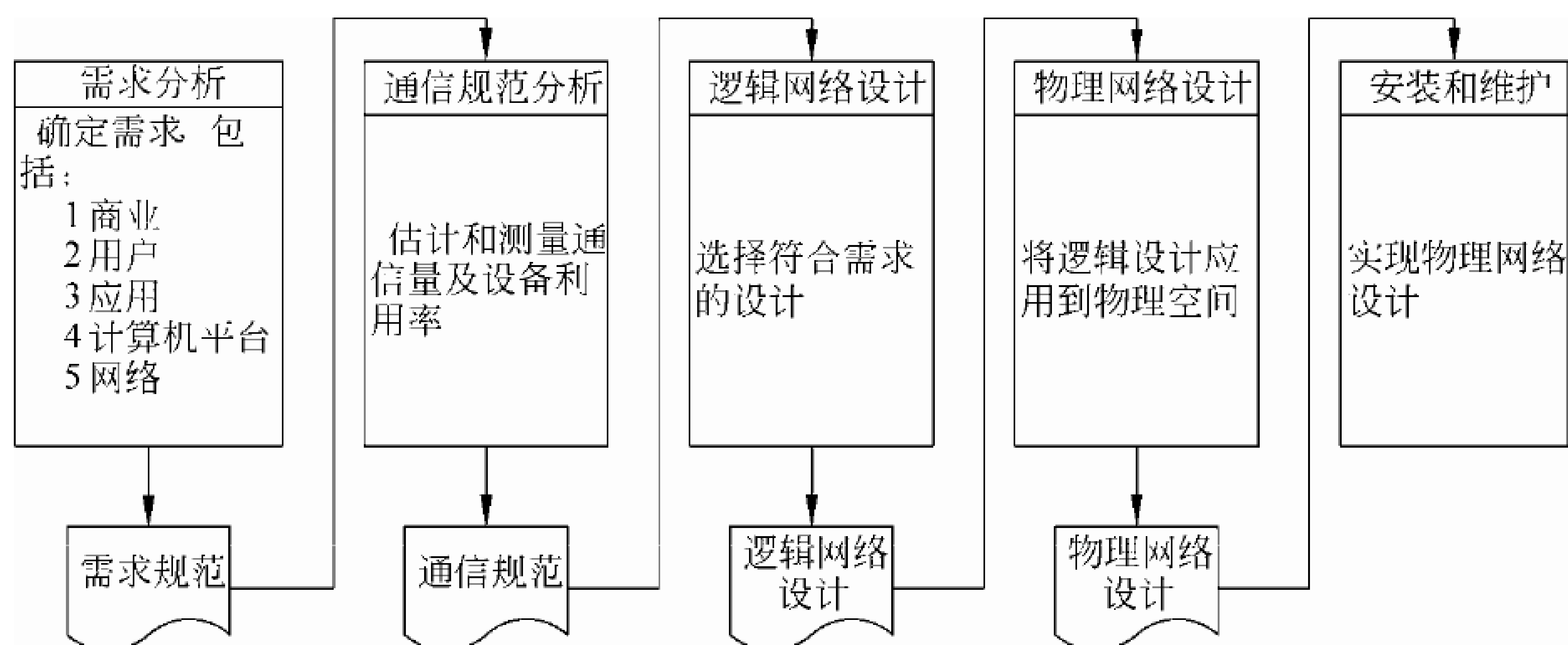
（69）A．网络 IP 地址分配方案　　B．设备列表清单
　　　C．集中访谈的信息资料　　D．网络内部的通信流量分布

（70）A．网络 IP 地址分配方案　　B．设备列表清单
　　　C．集中访谈的信息资料　　D．网络内部的通信流量分布

**试题（69）、（70）分析**

一个网络系统从构思开始，到最后被淘汰的过程称为网络生命周期。一般来说，网络生命周期应包括系统的构思和计划、分析和设计，以及运行和维护的全过程。网络系统的生命周期是一个循环迭代的过程，每次迭代的动力都来自于网络应用需求的变更。每一个迭代周期都是网络重构的过程。常见的迭代周期构成可分为以下阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

根据五阶段迭代周期的模型，每个阶段都必须依据上一阶段的成果，完成本阶段的工作，并形成本阶段的工作成果，作为下一阶段的工作依据。这些阶段成果分别为需求规范、通信规范、逻辑网络设计和物理网络设计文档。网络开发过程可以用下图来描述。




本题中的 4 个选项分别属于不同阶段的文档，其中：

A．网络 IP 地址分配方案：　　逻辑网络设计文档

B．设备列表清单：　　　　　物理网络设计文档

C．集中访谈的信息资料：　　需求规范文档

D．网络内部的通信流量分布：通信规范文档

**参考答案**

（69）A　（70）B

**试题（71）～（75）**

A transport layer protocol usually has several responsibilities. One is to create a process-to-process communication; UDP uses __(71)__ numbers to accomplish this. Another responsibility is to provide control mechanisms at the transport level. UDP does this task at a very minimal level. There is no flow control mechanism and there is no __(72)__ for received packet. UDP, however, does provide error control to some extent. If UDP detects an error in the received packet, it silently drop it.

The transport layer also provides a connection mechanism for the processes. The __(73)__ must be able to send streams of data to the transport layer. It is the responsibility of the transport layer at __(74)__ station to make the connection with the receiver, chop the stream into transportable units, number them, and send them one by one. It is the responsibility of the transport layer at the receiving end to wait until all the different units belonging to the same process have arrived, check and pass those that are __(75)__ free, and deliver them to the receiving process as a stream.

（71）A．hop　　B．port　　C．route　　D．packet

（72）A．connection　　B．window　　C．acknowledgement　　D．destination

（73）A．jobs　　B．processes　　C．programs　　D．users

（74）A．sending　　B．routing　　C．switching　　D．receiving

（75）A．call　　B．state　　C．cost　　D．error

**参考译文**

传输层协议通常有几个功能，其中之一就是生成进程与进程之间的通信。UDP 使用端口号来实现这个功能。另外一个责任是在传输级实现控制机制。UDP 对于这个任务只做很少的工作。没有流量控制，对于接收到的报文也没有应答。然而，UDP 在一定程度上还是做了差错控制工作。如果 UDP 在收到的报文中检测到了错误，就直接丢弃之。

传输层也提供进程之间的连接机制。进程应该能够向传输层发送数据流。与接收站建立连接是发送方传输层的责任，同时把数据流划分成可传输的单元，对其进行编号，然后一个接一个地发送它们。接收方传输层的责任就是等待属于同一进程的各个传输单元到达，检查其正确性，让没有错误的通过，并将其组织成数据流提交给接收进程。

**参考答案**

（71）B （72）C （73）B （74）A （75）D

# 第 12 章　2011 下半年网络工程师下午试题分析与解答

**试题一**（共 **15** 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某学校计划部署校园网络，其建筑物分布如图 1-1 所示。

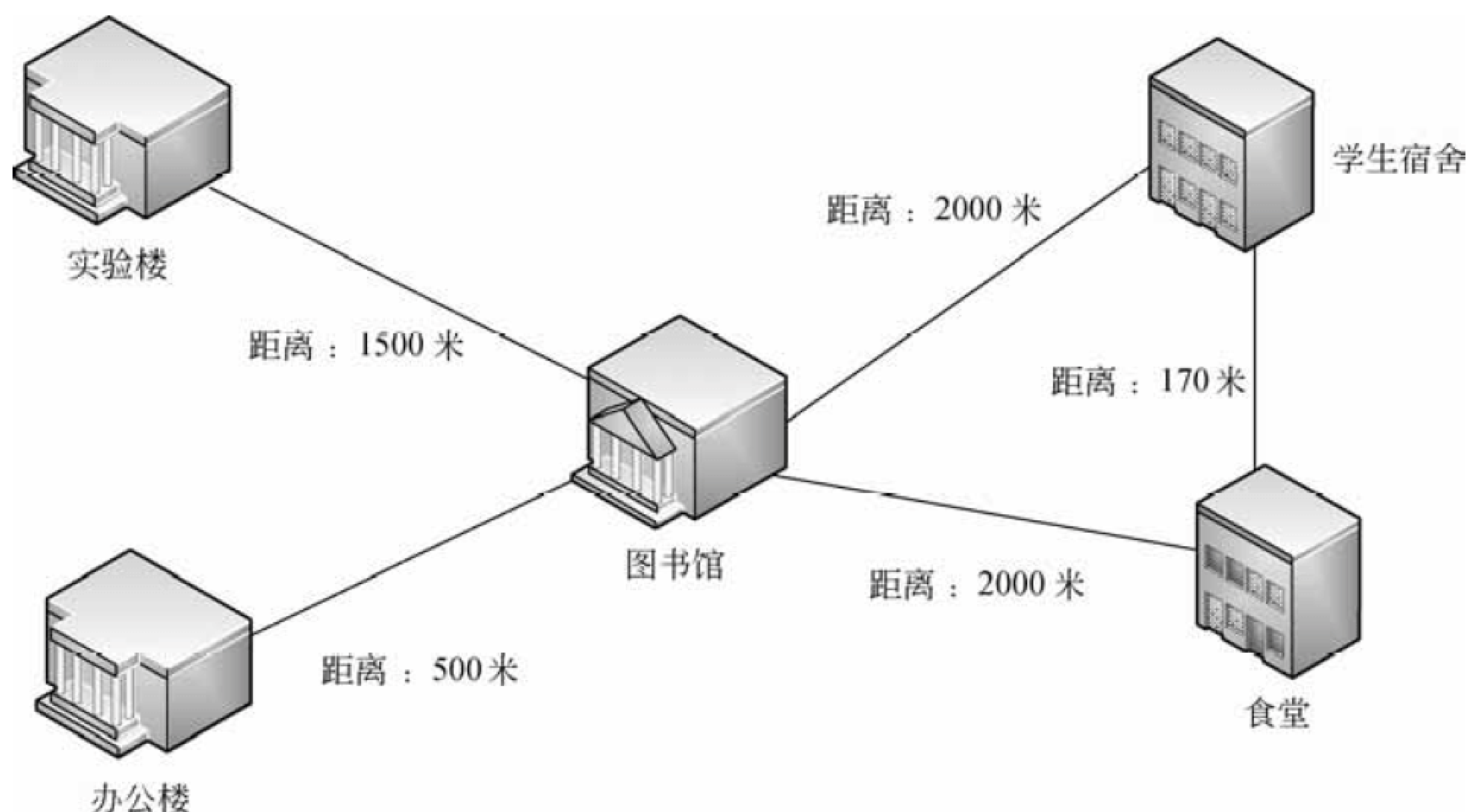



图 1-1

根据需求分析结果，校园网规划要求如下：

1．信息中心部署在图书馆。

2．实验楼部署 237 个点，办公楼部署 87 个点，学生宿舍部署 422 个点，食堂部署 17 个点。

3．为满足以后应用的需求，要求核心交换机到汇聚交换机以千兆链路聚合，同时千兆到桌面。

4．学校信息中心部署服务器，根据需求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务。

5．部署流控网关对 P2P 流量进行限制，以保证正常上网需求。

**【问题 1】**（**5** 分）

根据网络需求，设计人员设计的网络拓扑结构如图 1-2 所示。

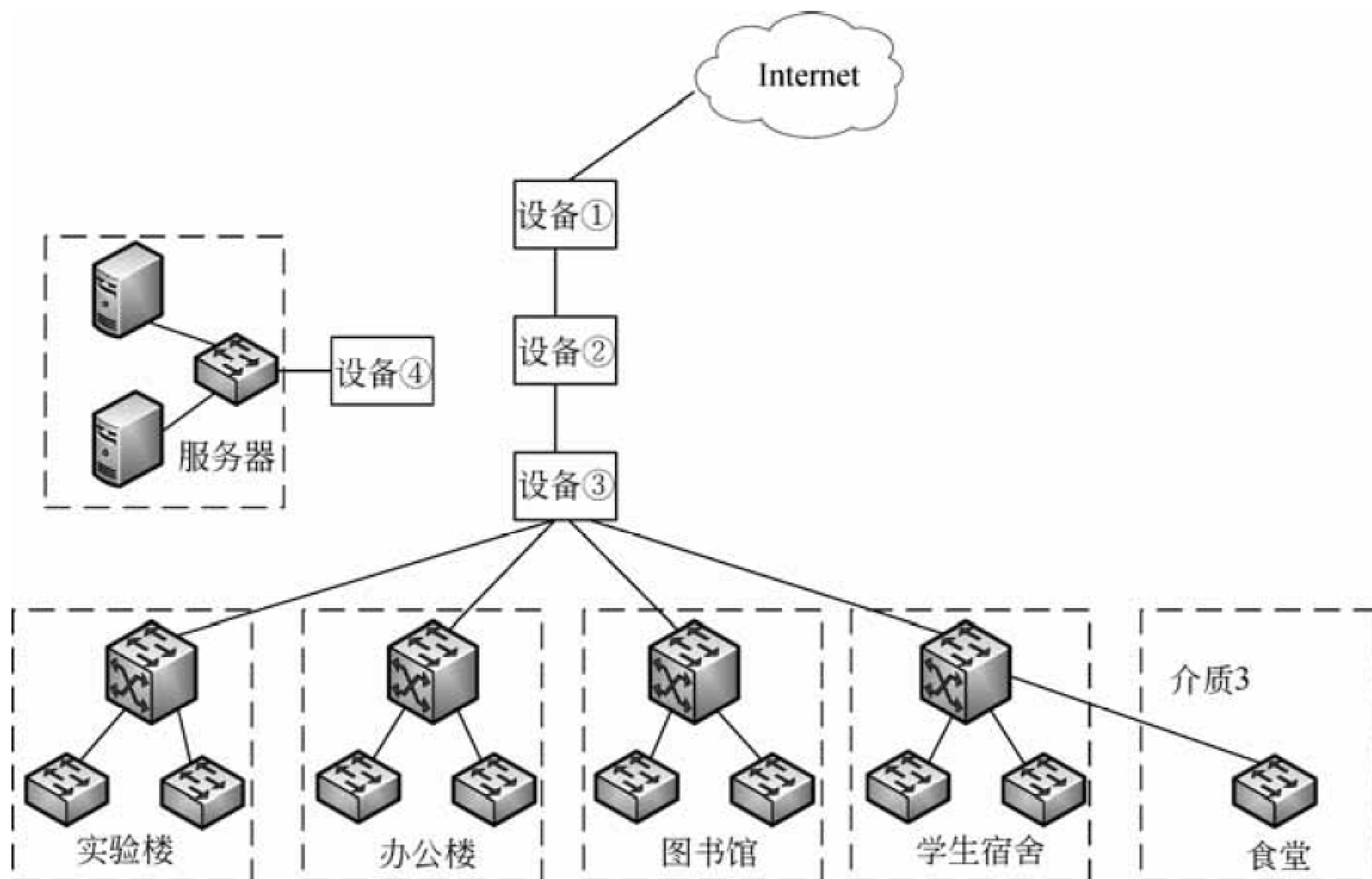



图 1-2

请根据网络需求描述和网络拓扑结构回答以下问题。

1．图 1-2 中设备①应为__（1）__，设备②应为__（2）__，设备③应为__（3）__，设备④应为__（4）__。

（1）～（4）备选答案：（每设备限选 1 次）

A．路由器　　B．核心交换机　　C．流控服务器　　D．防火墙

2．设备④应该接在设备__（5）__上。

**【问题 2】**（4 分）

1．根据题目说明和网络拓扑图，在图 1-2 中，介质 1 应选用__（6）__，介质 2 应选用__（7）__，介质 3 应选用__（8）__。

（6）～（8）备选答案：（注：每项只能选择一次）

A．单模光纤　　B．多模光纤

C．6 类双绞线　　D．5类双绞线

2．根据网络需求分析和网络拓扑结构图，所有接入交换机都直接连接汇聚交换机，本校园网中至少需要__（9）__台 24 口的接入交换机（不包括服务器使用的交换机）。

**【问题 3】**（4 分）

交换机的选型是网络设计的重要工作。而交换机的背板带宽、包转发率、交换容量是其重要技术指标。其中，交换机进行数据包转发的能力称为__（10）__，交换机端口处理器和数据总线之间单位时间内所能传输的最大数据量称为__（11）__。某交换机有 24 个固定的千兆端口，其端口总带宽为__（12）__Mbps。

**【问题 4】（2 分）**

根据需求分析，图书馆需要支持无线网络接入，其部分交换机需要提供 POE 功能，POE 的标准供电电压值为__（13）__。

（13）备选答案：

A. 5V　B. 12V　C. 48V　D. 110V

**试题一分析**

本题考查园区网络部署的基本知识。要求考生结合自己掌握的传输介质、网络设备、服务器等知识，根据实际项目需求，完成网络部署方案的设计。

**【问题 1】**

本问题考查网络设备选型及部署的能力。

由题目给出的需求分析结果及校园网规划要求可知，该网络采用了三层架构部署。由拓扑图 1-2 可知，设备①直接连接 Internet，在可选的四个设备中，在此位置可选择的设备可以是路由器或防火墙，但是由于每个设备只能选择一次，而需求说明中提到“学校信息中心部署服务器，根据需求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务”，所以可以判断设备④应为防火墙，所以设备①应为路由器。由于该网络采用三层架构，所以设备③直接连接多台汇聚交换机，该设备应为核心交换机，剩下的设备②直连在路由器与核心交换机之间，按照需求分析和设备选项，这里应该部署流控服务器。

根据以上分析可知，设备④应为防火墙，由于服务器要对内外网分别提供不同的服务，根据网络拓扑结构，防火墙设备连接在核心交换机上最适合。

**【问题 2】**

本问题考查网络传输介质的选择能力。

由需求分析可知，信息中心部署在图书馆，核心交换机到汇聚交换机以千兆链路聚合，接入交换机千兆到桌面。同时由图 1-1 可知，图书馆到实验楼的距离为 1500 米，所以介质 1 应选择单模光纤；由图 1-2 可知，食堂的接入交换机上联到学生宿舍的汇聚交换机，距离为 170 米，所以介质 3 应选择光纤，而介质 1 必须选择单模光纤，题目要求每项只能选择一次，所以介质 3 应选择多模光纤。介质 2 只剩下 6 类双绞线和 5 类双绞线两个选项，由于需求要求千兆到桌面，所以此处合适的介质只能选择 6 类双绞线。

由需求可知，实验楼部署 237 个点，办公楼部署 87 个点，学生宿舍部署 422 个点，食堂部署 17 个点，如果采用 24 口的接入交换机，所有接入交换机都直接连接汇聚交换机，则每个交换机可用 23 个端口，这样实验楼需部署 11 个；办公楼部署 4 个；学生宿舍部署 19 个；食堂部署 1 个；合计 35 个。

**【问题 3】**

本问题考查交换机基本参数的知识。

交换机的选型是网络设计的重要工作。而交换机的背板带宽、包转发率、交换容量

是其重要技术指标。

其中，交换机进行数据包转发的能力称为包转发率，也称端口吞吐率，指交换机进行数据包转发的能力，单位为 pps（package per second）。

交换机的背板带宽是指交换机端口处理器和数据总线之间单位时间内所能传输的最大数据量。背板带宽标志了交换机总的交换能力，单位为 Gb/s。一般交换机的背板带宽从几个 Gb/s 到上百个 Gb/s。

交换机所有端口能提供的总带宽的计算公式为：

总带宽＝端口数×端口速率×2（全双工模式）

如果某交换机有 24 个固定的千兆端口，其端口总带宽=24×1000×2=48000Mbps

**【问题 4】分析**

本问题考查 POE 的基础知识。

POE（Power over Ethernet）称为以太网供电，其可以通过双绞线为以太网提供 48V 的交流电源。

**参考答案**

**【问题 1】**

1.（1）A 路由器　（2）C 流控服务器　（3）B 核心交换机　（4）D 防火墙

2.（5）核心交换机 （或 B 或 设备③）

**【问题 2】**

1.（6）A 单模光纤　（7）C　6 类双绞线　（8）B 多模光纤

2.（9）35

**【问题 3】**

（10）包转发率

（11）背板带宽

（12）48000

**【问题 4】**

（13）C　48V

**试题二（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

如图 2-1 所示，某公司办公网络划分为研发部和销售部两个子网，利用一台双网卡 Linux 服务器作为网关，同时在该 Linux 服务器上配置 Apache 提供 Web 服务。

**【问题 1】（4 分）**

图 2-2 是 Linux 服务器中网卡 eth0 的配置信息，从图中可以得知：①处输入的命令是__（1）__，eth0 的 IP 地址是__（2）__，子网掩码是__（3）__，销售部子网最多可以容纳的主机数量是__（4）__。

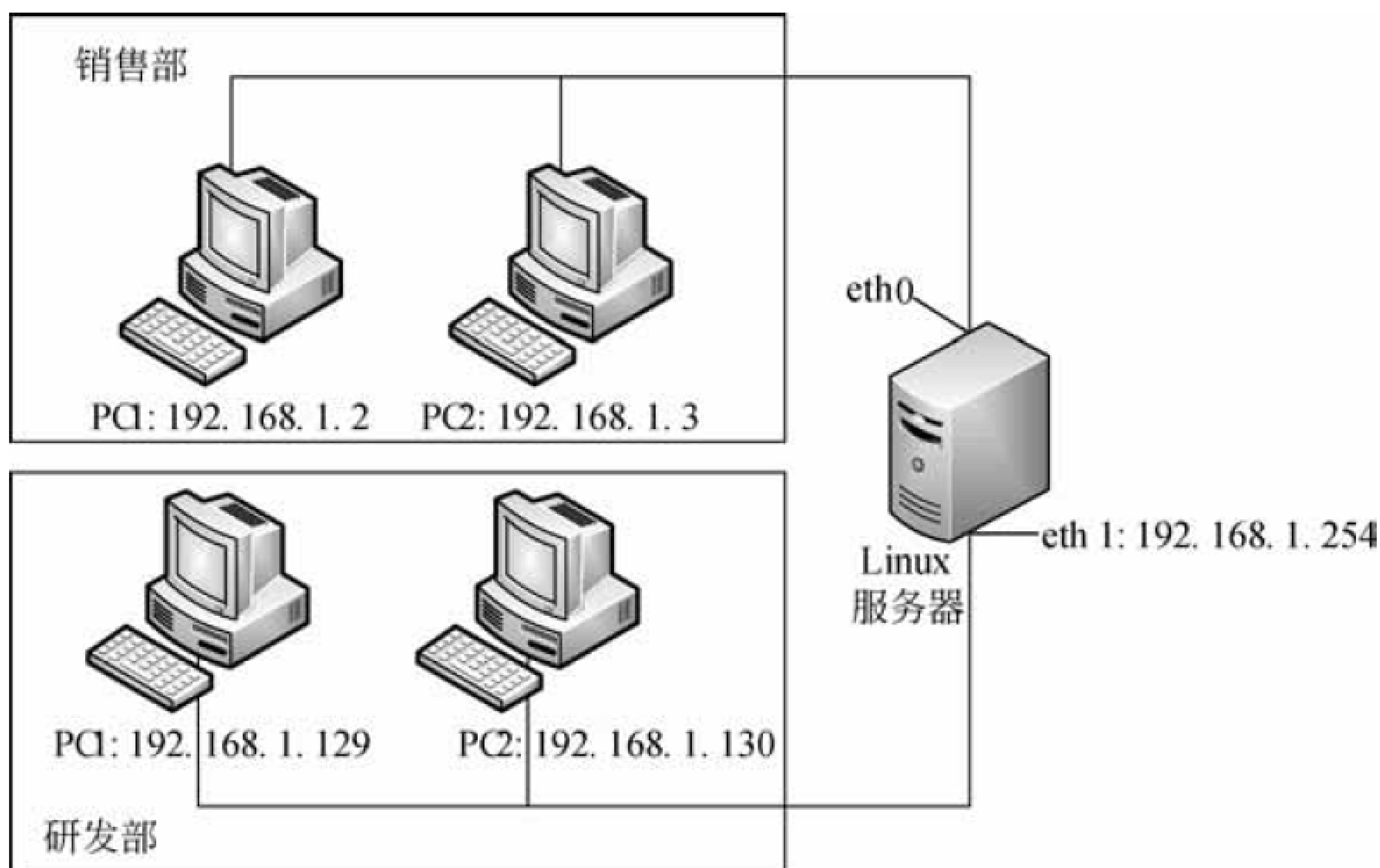



图 2-1

```
[root@localhost conf]#____①____
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C8:0D:10
          inet addr:192.168.1.126  Bcast:192.168.1.255  Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1667 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:291745 (284.9 Kb)  TX bytes:924 (924.0 b)
          Interrupt:10 Base address:0x10a4
```

图 2-2

**【问题 2】（4 分）**

Linux 服务器配置 Web 服务之前，执行命令[root@root] rpm -qa | grep httpd 的目的是 （5）。Web 服务器配置完成后，可以用命令 （6） 来启动 Web 服务。

**【问题 3】（3 分）**

缺省安装时，Apache 的主配置文件名是 （7），该文件所在目录为 （8）。

配置文件中下列配置信息的含义是 （9）。

```
<Directory "/var/www/html/secure">
AllowOverride AuthConfig
Order deny,allow
Allow from 192.168.1.2
Deny from all
</Directory>
```

**【问题 4】（4 分）**

Apache 的主配置文件中有一行：Listen 192.168.1.126:80，其含义是__（10）__。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务。在 Linux 服务器中应如何配置，方能使研发部的主机也可以访问 Web 服务。

**试题二分析**

本题考查 Linux 服务器相关的配置。

**【问题 1】**

Linux 系统中，采用 ifconfig 命令可以查看网卡的配置信息，ifconfig 命令加上网卡的名称，可以指定需要查看的网卡。

从 eth0 网卡配置信息中可以知道网卡的 IP 地址为 192.168.1.126，子网掩码为 255.255.255.128。从子网掩码可以看出该网段可以容纳的主机数量为 126 台，如果除去 Linux 服务器占用的一个地址，则答案为 125 台。

**【问题 2】**

Linux 命令 rpm -qa 用于查看系统安全的软件包，如果系统安装了 Apache，就包含 httpd 文件。所以该命令可用来检查 Apache 是否安装成功。

Linux 中启动某服务的命令是 service xxx start。所以用 service httpd start 来启动 Web 服务。

**【问题 3】**

Apache 缺省的主配置文件名是 httpd.conf，该文件所在目录为/etc/httpd/conf。

目录“/var/www/html/secure”的配置信息表明该目录只允许主机 192.168.1.2 访问。

**【问题 4】**

Apache 的主配置文件中有配置项 Listen　ip:port 的含义是指定服务在某个 IP 地址和端口上提供。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务，表明研发部无法访问 192.168.1.126 这个 IP 地址，解决方法是增加从研发部网络到销售部网络的路由配置或者更改配置项 Listen　ip:port 为不指定 IP 地址，则研发部网络可以通过 192.168.1.254 访问 Web 服务。

**参考答案**

**【问题 1】**

（1）ifconfig eth0　或　ifconfig

（2）192.168.1.126

（3）255.255.255.128

（4）125（答 126 也正确）

**【问题 2】**

（5）确认 Apache 软件包是否已经成功安装

（6）service httpd start

【问题 3】

（7）httpd.conf

（8）/etc/httpd/conf

（9）目录“/var/www/html/secure”只允许主机 192.168.1.2 访问。

【问题 4】

（10）提供 Web 服务的地址是 192.168.1.126，端口是 80

将 Apache 的主配置文件中配置“Listen 192.168.1.126:80” 修改为“Listen 80”，或者增加从研发部网络到销售部网络的路由。

**试题三（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

在 Windows Server 2003 中可以采用筛选器来保护 DNS 通信。某网络拓扑结构如图 3-1 所示。WWW 服务器的域名是 www.abc.edu。DNS 服务器上安装 Windows Server 2003 操作系统。

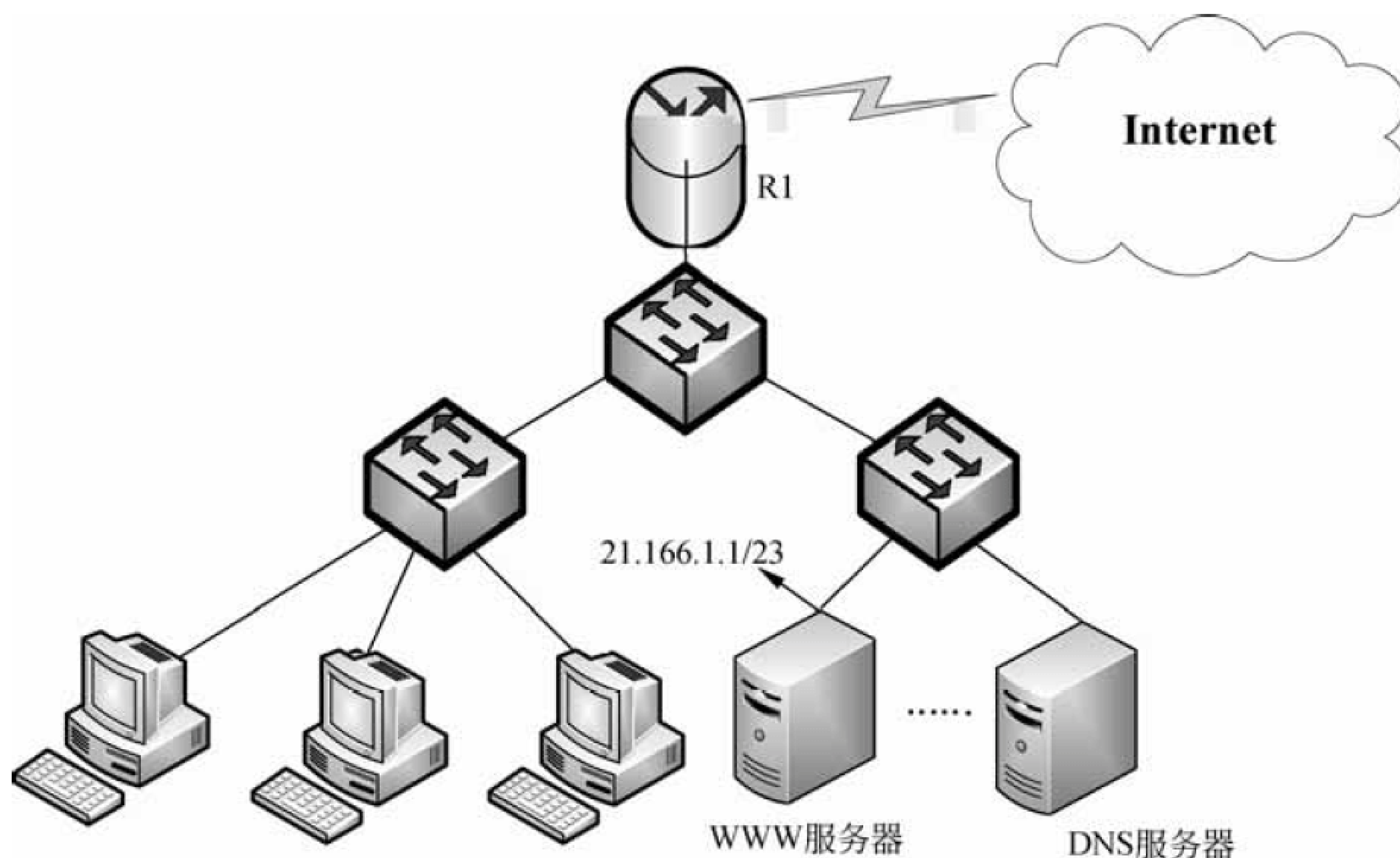



图 3-1

【问题 1】（3 分）

配置 DNS 服务器时，在图 3-2 所示的对话框中，为 Web Server 配置记录时新建区域的名称是__（1）__；在图 3-3 所示的对话框中，添加的新建主机“名称”为__（2）__，IP 地址栏应填入__（3）__。

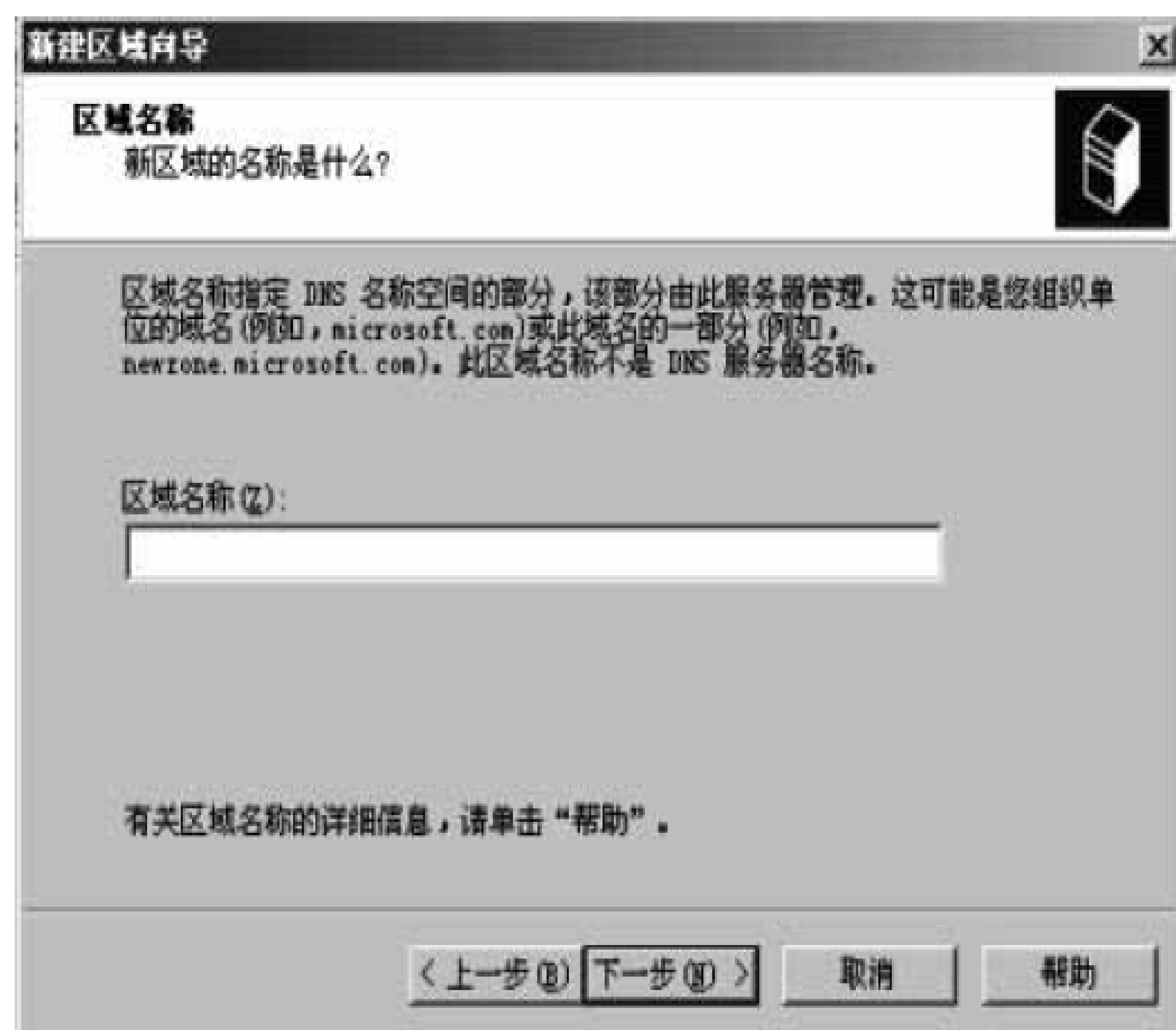



图 3-2

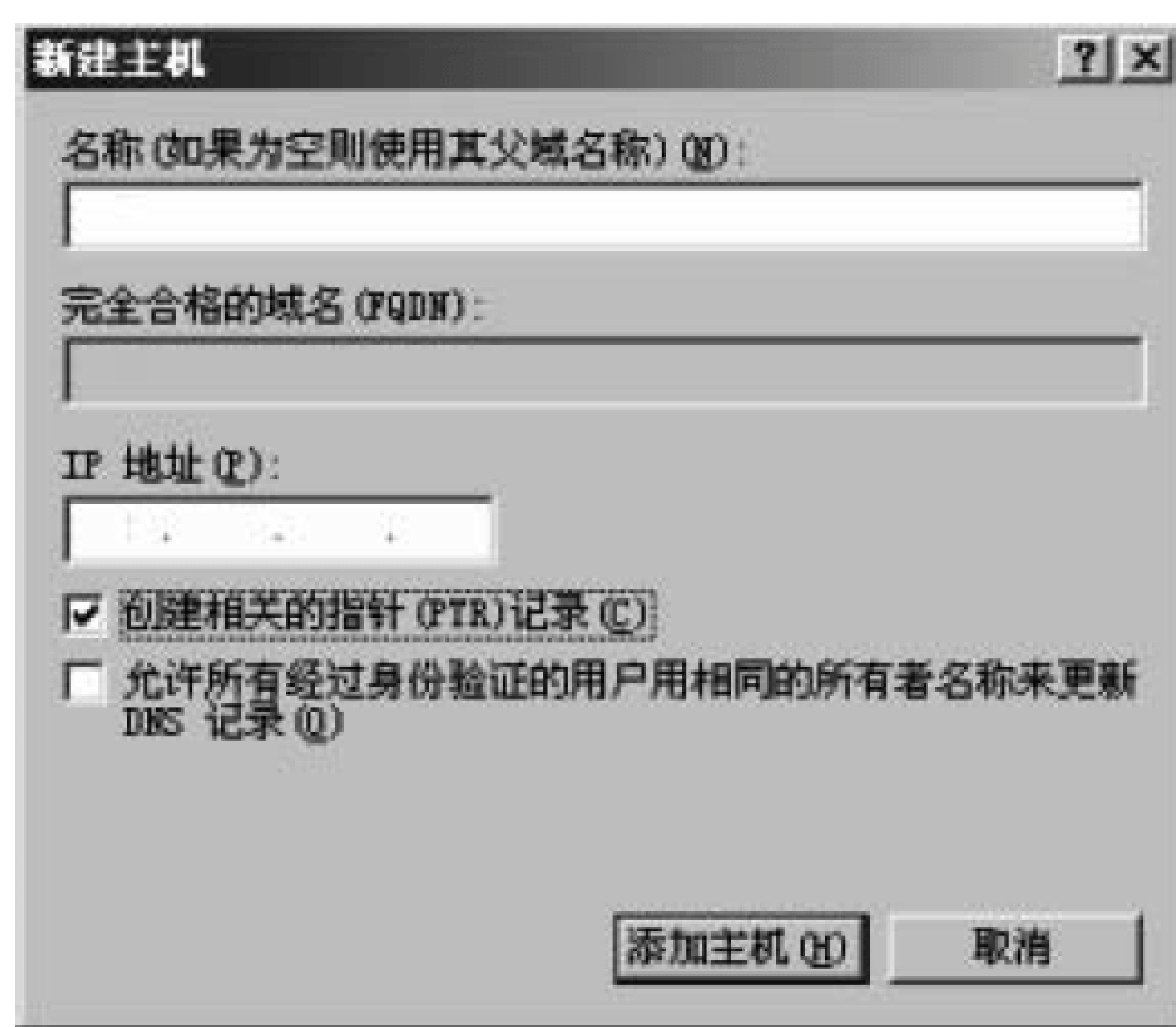



图 3-3

**【问题 2】（4 分）**

在 DNS 服务器的“管理工具”中运行“管理 IP 筛选器列表”，创建一个名为“DNS 输入”的筛选器，用以对客户端发来的 DNS 请求消息进行筛选。在如图 3-4 所示的“IP 筛选器向导”中指定 IP 通信的源地址，下拉框中应选择__（4）__；在如图 3-5 中指定 IP 通信的目标地址，下拉框中应选择__（5）__。

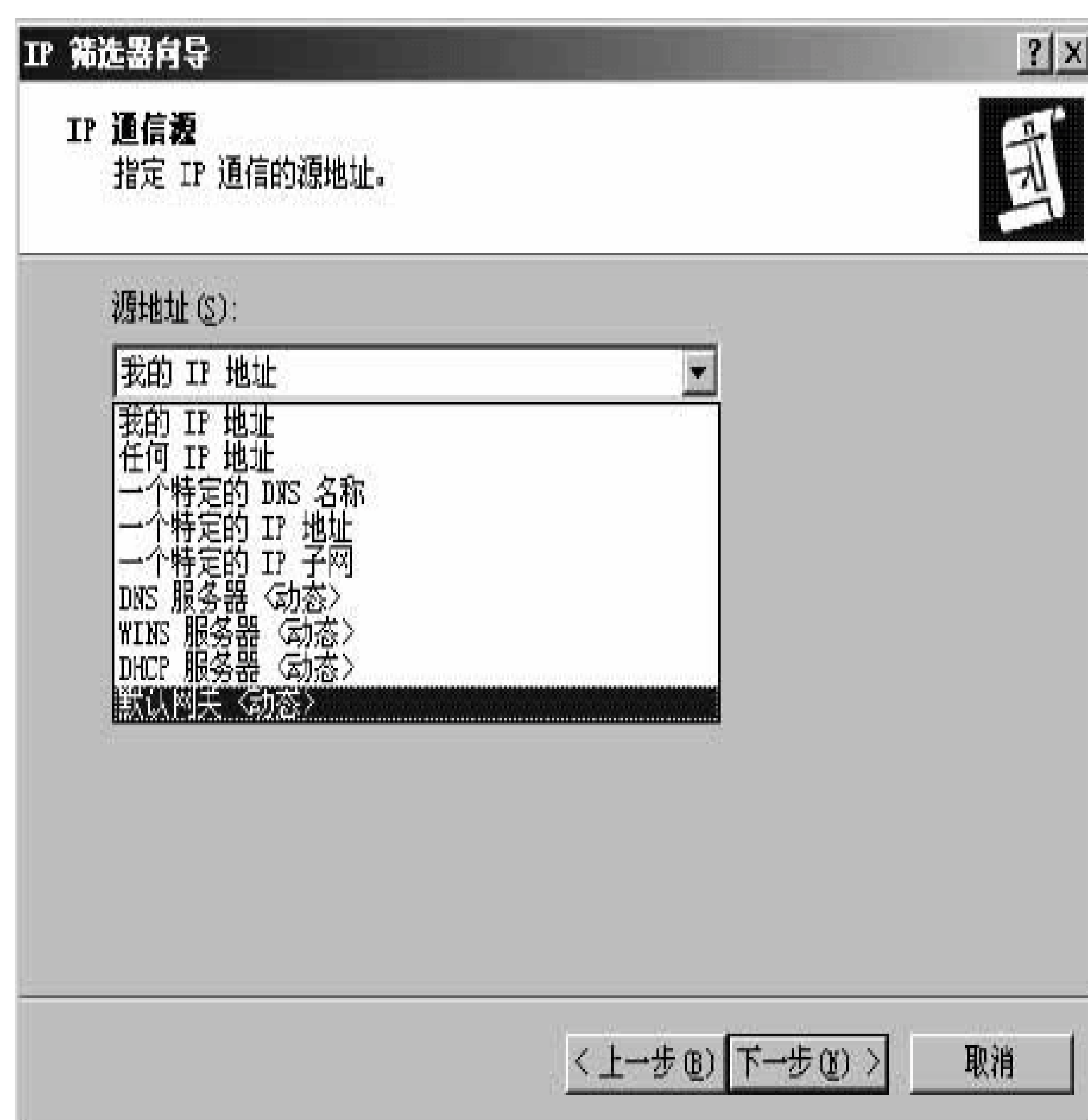



图 3-4




图 3-5

在图 3-6 中源端口项的设置方式为__（6）__，目的端口项的设置方式为__（7）__。在筛选器列表配置完成后，设置“筛选器操作”为“允许”。

**【问题 3】（2 分）**

在图 3-7 中双击“新 IP 安全策略”即可查看“DNS 输入”安全规则，要使规则生

效，在图 3-7 中如何配置？

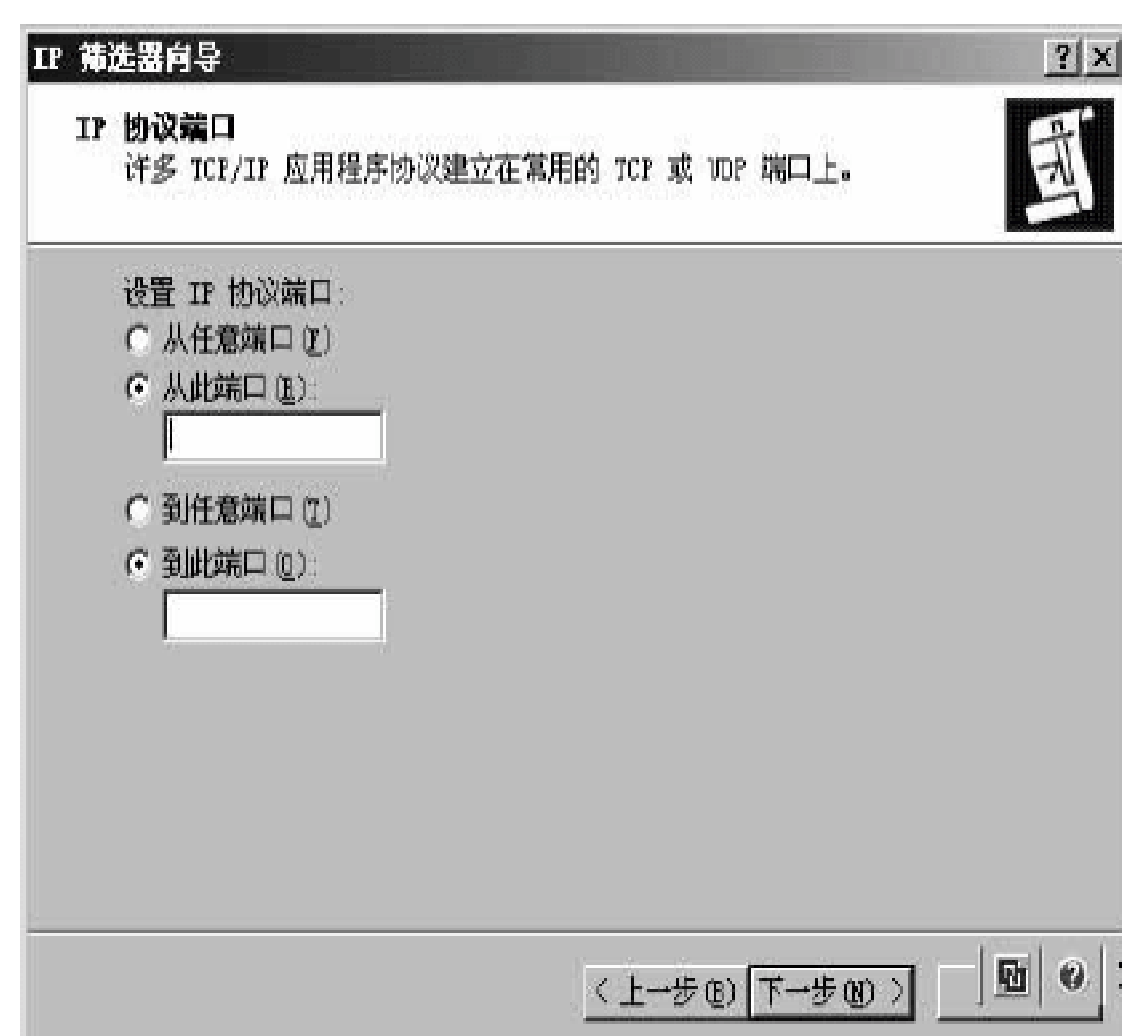



图 3-6




图 3-7

**【问题 4】**（6 分）

在本机 Windows 命令行中输入__（8）__命令可显示当前 DNS 缓存，如图 3-8 所示。"Record Type" 字段中的值为 4 时存储的记录是 MX，若 "Record Type" 字段中的值为 2 时存储的记录是__（9）__。

客户端在排除 DNS 域名解析故障时需要刷新 DNS 解析器缓存，使用的命令是__（10）__。

```
Windows IP Configuration

    aaa.bbb.com
    ----------------------------------------
    Record Name . . . . . : aaa.bbb.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 353
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 217.141.248.156

    w.ccc.com
    ----------------------------------------
    Record Name . . . . . : w.ccc.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 38
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    CNAME Record  . . . . : cache.ccc.com
```

图 3-8

## 试题三分析

本题考查 Windows Server 2003 筛选器和 DNS 配置相关知识。

【问题 1】

配置 DNS 服务器解析记录时，新建区域即记录主机所在域的名称，主机名称是该域中主机的标识，IP 地址为记录主机的 IP 地址，故（1）～（3）依次应填入 abc.edu、www 和 221.166.1.1。

【问题 2】

在创建客户端发来的 DNS 请求消息筛选器时，源地址为客户端的 IP 地址，故（4）处应选“任何 IP 地址”；目标地址处为 DNS 服务器的 IP 地址，故（5）处应选“我的 IP 地址”。源端口项为客户端的端口号，应为任意高端，故（6）处应点击“从任意端口”，目的端口项是 DNS 服务的端口号，故设置方式为点击“到此端口”，文本框中填入“53”。

【问题 3】

要使规则生效，需要对指派规则，故右键单击“新 IP 安全策略”，点击“指派”。

【问题 4】

要显示当前 DNS 缓存，可在本机 Windows 命令行中输入 ipconfig/displaydns；若“Record Type”字段中的值为 2 时存储的记录是 IP 地址对应的域名，即反向解析。客户端在排除 DNS 域名解析故障时需要刷新 DNS 解析器缓存，使用的命令是 ipconfig/flushdns。

**参考答案**

【问题 1】

（1）abc.edu

（2）www

（3）221.166.1.1

【问题 2】

（4）任何 IP 地址

（5）我的 IP 地址

（6）点击“从任意端口”

（7）点击“到此端口”，文本框中填入“53”

【问题 3】

右键单击“新 IP 安全策略”，点击“指派”

【问题 4】

（8）ipconfig/displaydns

（9）IP 地址对应的域名（反向解析）

（10）ipconfig/flushdns

**试题四（共 15 分）**

阅读下列关于路由器配置的说明，回答问题 1 至问题 5，将答案填入答题纸对应的解答栏内。

**【说明】**

某公司网络结构如图 4-1 所示，通过在路由器上配置访问控制列表 ACL 来提高内部网络和 Web 服务器的安全。

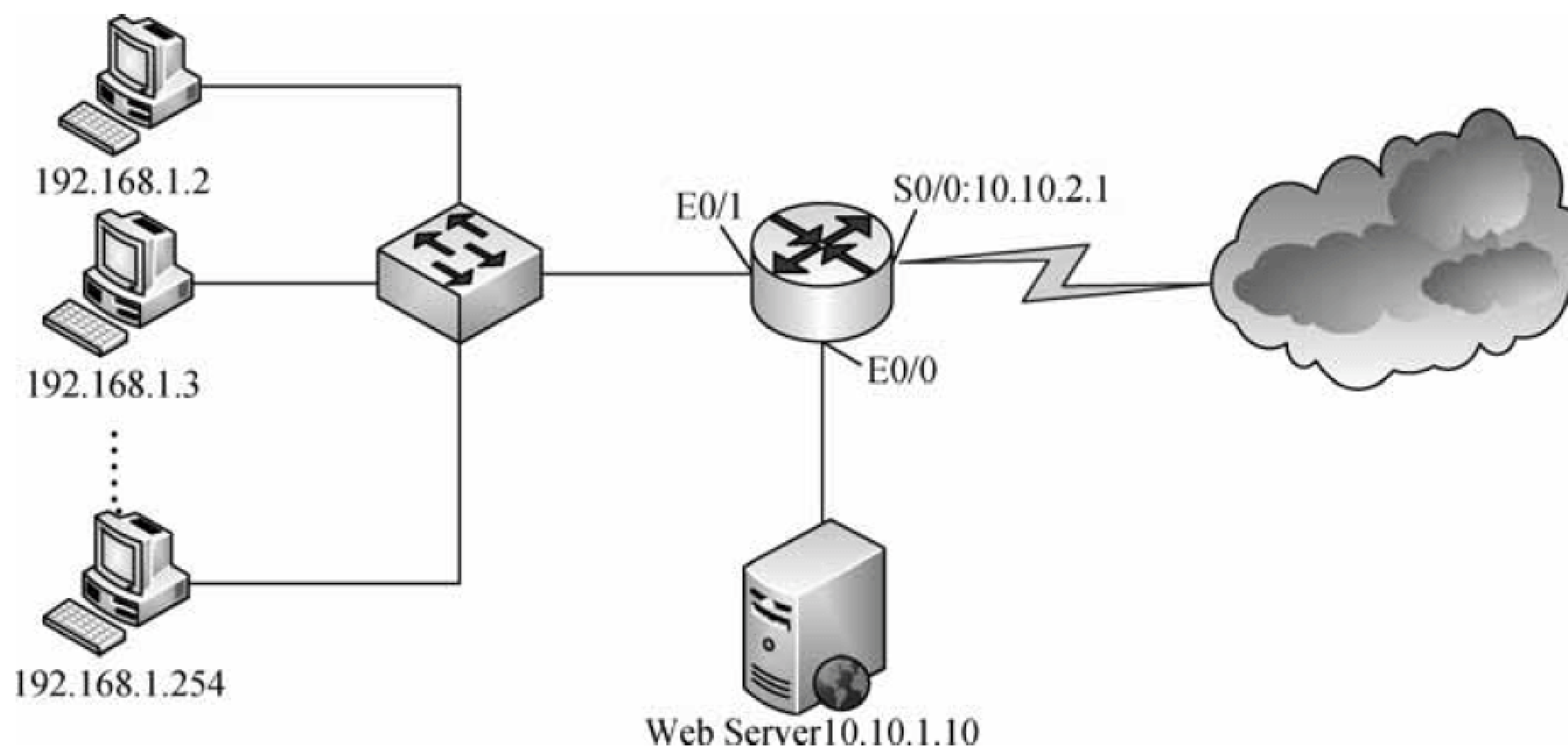



图 4-1

**【问题 1】（2 分）**

访问控制列表（ACL）对流入/流出路由器各端口的数据包进行过滤。ACL 按照其功能分为两类，__（1）__只能根据数据包的源地址进行过滤，__（2）__可以根据源地址、目的地址以及端口号进行过滤。

**【问题 2】（3 分）**

根据图 4-1 的配置，补充完成下面路由器的配置命令：

```
    Router(config)# interface  (3)
    Router(config-if)#ip address 10.10.1.1  255.255.255.0
    Router(config-if)#no shutdown
    Router(config-if)#exit
    Router(config)# interface  (4)
    Router(config-if)# ip address 192.168.1.1  255.255.255.0
…
Router(config)# interface  (5)
    Router(config-if)# ip address 10.10.2.1  255.255.255.0
…
```

**【问题 3】（4 分）**

补充完成下面的 ACL 语句，禁止内网用户 192.168.1.254 访问公司 Web 服务器和外网。

```
    Router(config)#access-list 1 deny  (6)
```

```
Router(config)#access-list 1 permit  any
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 1 __(7)__
```

**【问题4】（3分）**

请说明下面这组ACL语句的功能。

```
Router(config)#access-list 101 permit tcp any host 10.10.1.10 eq www
Router(config)#interface ethernet 0/0
Router(config-if)#ip access-group 101 out
```

**【问题5】（3分）**

请在问题4的ACL前面添加一条语句，使得内网主机192.168.1.2可以使用telnet对Web服务器进行维护。

```
Router(config)#access-list 101 __(8)__
```

**试题四分析**

本题考查访问控制列表ACL相关的配置。

**【问题1】**

访问控制列表（ACL）对流入/流出路由器各端口的数据包进行过滤。ACL按照其功能分为两类，标准ACL只能根据数据包的源地址进行过滤，扩展ACL可以根据源地址、目的地址以及端口号进行过滤。

**【问题2】**

根据图4-1的配置可知，E0/1接口对应192.168.1.1/24网段，该网段只有地址192.168.1.1可用，S0/0对应的IP地址是10.10.2.1，E0/0对应10.10.1.1/24网段。所以（3）～（5）处应分别填入e 0/0、e 0/1、s 0/0。

**【问题3】**

禁止内网用户192.168.1.254访问公司Web服务器和外网，可以采用标准ACL在E0/1接口禁止源地址为192.168.1.254的包进入路由器接口。所以（6）处应为192.168.1.254，（7）处应为in。

**【问题4】**

"permit tcp any host 10.10.1.10 eq www"为允许任何主机访问10.10.1.10的WWW服务。

**【问题5】**

扩展ACL的语法如下：

```
access-list 100-199|2000-2699 permit|deny protocol
source_address source_wildcard_mask [protocol_information]
destination_address destination_wildcard_mask [protocol_information] [log]
```

所以内网主机 192.168.1.2 使用 telnet 对 Web 服务器进行维护的 ACL 语句应该为“permit tcp host 192.168.1.2　host 10.10.1.10 eq telnet”。

**参考答案**

**【问题 1】**

（1）标准 ACL

（2）扩展 ACL

**【问题 2】**

（3）ethernet 0/0　（e 0/0）

（4）ethernet 0/1　（e 0/1）

（5）serial 0/0（s 0/0）

**【问题 3】**

（6）192.168.1.254

（7）in

**【问题 4】**

允许任何主机访问公司内部的 Web 服务。

**【问题 5】**

permit tcp host 192.168.1.2　host 10.10.1.10 eq telnet

（host ×.×.×.×可以写成×.×.×.× 0.0.0.0，telnet 可以写成 23）

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位在实验室部署了 IPv6 主机，在对现有网络不升级的情况下，计划采用 NAT-PT 方式进行过渡，实现 IPv4 主机与 IPv6 主机之间的通信，其网络结构如图 5-1 所示。其中，IPv6 网络使用的 NAT-PT 前缀是 2001:aaaa:0:0:0:1::/96，IPv6 网络中的任意结点动态映射到地址池 16.23.31.10～16.23.31.20 中的 IPv4 地址。

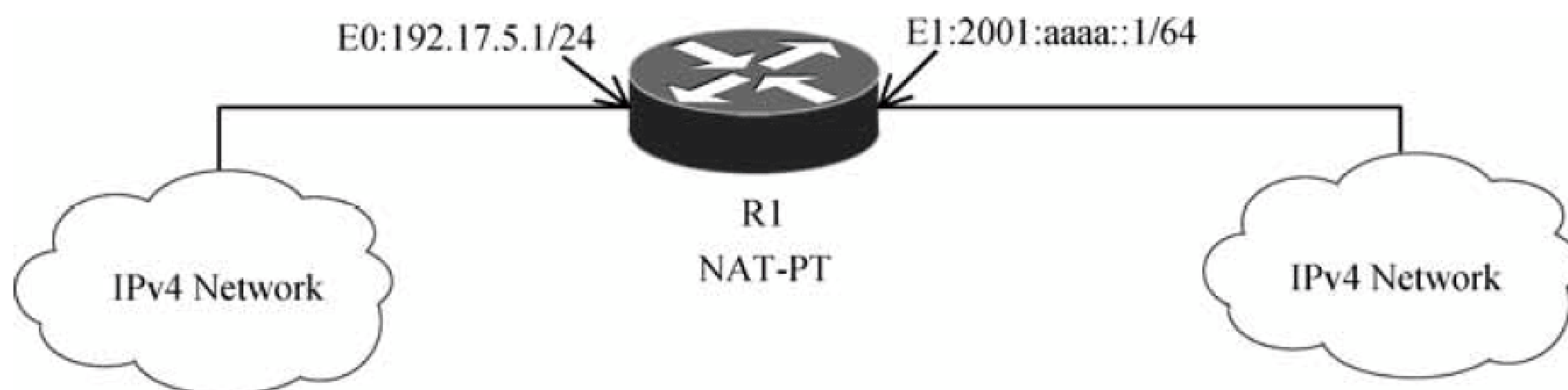



图 5-1

**【问题 1】（4 分）**

使用 NAT-PT 方式完成 IPv4 主机与 IPv6 主机通信，需要路由器支持，在路由器上需要配置 DNS-ALG 和 FTP-ALG 这两种常用的应用网关。

没有 DNS-ALG 和 FTP-ALG 的支持，无法实现__(1)__结点发起的与__(2)__结点之间的通信。

**【问题 2】（8 分）**

根据网络拓扑和需求说明，完成（或解释）路由器 R1 的配置。

```
R1 # configure terminal                                  ;进入全局配置模式
R1(config) # interface ethernet0                         ;进入端口配置模式
R1(config-if) # ip address __(3)__ __(4)__               ;配置端口 IP 地址
R1(config-if) # ipv6 nat                                 ; __(5)__
…
R1(config-if) # interface ethernet1
R1(config-if) # ipv6 address __(6)__/64
R1(config-if) # ipv6 nat
…
R1(config) #ipv6 access-list ipv6 permit 2001:aaaa::1/64 any   ; __(7)__
R1(config) #ipv6 nat prefix __(8)__
R1(config) #ipv6 nat v6v4 pool ipv4-pool __(9)__ __(10)__ prefix-length 24
R1(config) #ipv6 nat v6v4 source list ipv6 pool ipv4-pool
R1(config) #exit
```

**【问题 3】（3 分）**

NAT-PT 机制定义了三种不同类型的操作，其中，__(11)__提供一对一的 IPv6 地址和 IPv4 地址的映射；__(12)__也提供一对一的映射，但是使用一个 IPv4 地址池；__(13)__提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。

**试题五分析**

本题考查采用 NAT-PT 方式实现 IPv4 主机与 IPv6 主机之间通信的基本知识。

**【问题 1】**

本问题考查考生掌握 NAT-PT 的基本知识的能力。

NAT-PT（Network Address Translation-Protocol）网络地址转换协议转换是一种纯 IPv6 结点和 IPv4 结点间的互通方式，所有包括地址、协议在内的转换工作都由网络设备来完成。支持 NAT-PT 的网关路由器应具有 IPv4 地址池，在从 IPv6 向 IPv4 域中转发包时使用，地址池中的地址是用来转换 IPv6 报文中的源地址的。此外网关路由器需要 DNS-ALG 和 FTP-ALG 这两种常用的应用层网关的支持，在 IPv6 结点访问 IPv4 结点时发挥作用。如果没有 DNS-ALG 的支持，只能实现由 IPv6 结点发起的与 IPv4 结点之间的通信，反之则不行。如果没有 FTP-ALG 的支持，IPv4 网络中的主机将不能用 FTP 软件从 IPv6 网络中的服务器上下载文件或者上传文件，反之亦然。

**【问题 2】**

本问题主要考查考生配置 NAT-PT 的能力。

根据题目的描述可知，在该配置中，IPv6 网络使用的 NAT-PT 前缀是 2001:aaaa:0:0:0:1::/96，IPv6 网络中的任意结点动态映射到地址池 16.23.31.10～16.23.31.20 中的 IPv4 地址。具体的端口地址见图 5-1。所以，其配置应为：

```
R1 # configure terminal                               ;进入全局配置模式
R1(config) # interface ethernet0                      ;进入端口配置模式
R1(config-if) # ip address  192.17.5.1  255.255.255.0   ;配置端口 IP 地址
R1(config-if) # ipv6 nat                              ;在接口上启用 NAT-PT
…
R1(config-if) # interface ethernet1
R1(config-if) # ipv6 address 2001:aaaa::1/64
R1(config-if) # ipv6 nat
…
R1(config) #ipv6 access-list ipv6 permit 2001:aaaa::1/64 any;
指定 IPv6 网络中允许被转换的 IPv6 地址范围
R1(config) #ipv6 nat prefix  2001:aaaa:0:0:0:1::/96
R1(config) #ipv6 nat v6v4 pool ipv4-pool  16.23.31.10  16.23.31.20  pref-
ix-length 24
R1(config) #ipv6 nat v6v4 source list ipv6 pool ipv4-pool
R1(config) #exit
```

**【问题 3】**

本问题考查 NAT-PT 机制定义了三种不同类型的操作。

NAT-PT 机制定义的以下不同类型的操作：

静态 NAT-PT：静态模式提供一对一的 IPv6 地址和 IPv4 地址的映射。IPv6 单协议网络内的结点要访问的 IPv4 单协议网络内的每一个 IPv4 地址都必须在 NAT-PT 设备中设置。每一个目的 IPv4 地址在 NAT-PT 设备中被映射为一个具有预定义 NAT-PT 前缀的 IPv6 地址。这种模式中，每一个 IPv6 到 IPv4 映射需要一个源 IPv4 地址。静态 NAT-PT 模式跟 IPv4 中的静态 NAT 类似。

动态 NAT-PT：动态模式也提供一对一的映射，但是使用一个 IPv4 地址池。池中的源 IPv4 地址数量决定了并发的 IPv6 到 IPv4 转换的最大数目。在 IPv6 网络中 IPv6 单协议网络结点动态地把预定义的 NAT-PT 前缀增加到目的 IPv4 地址。这种模式需要一个 IPv4 地址池来执行动态的地址转换，动态 NAT-PT 模式和 IPv4 中的动态 NAT 类似。

NAPT-PT：网络地址端口转换协议转换，NAPT-PT 提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。这种转换同时在第 3 层（IPv4/IPv6）和上层（TCP/UDP）进行。NAPT-PT 和 IPv4 中的 PAT 转换类似。

## 参考答案

**【问题 1】**

（1）IPv4

（2）IPv6

**【问题 2】**

（3）192.17.5.1

（4）255.255.255.0

（5）在接口上启用 NAT-PT

（6）2001:aaaa::1

（7）指定 IPv6 网络中允许被转换的 IPv6 地址范围

（8）2001:aaaa:0:0:0:1::/96

（9）16.23.31.10

（10）16.23.31.20

**【问题 3】**

（11）静态模式

（12）动态模式

（13）NAPT-PT（网络地址端口转换协议转换）

# 第 13 章　2012 上半年网络工程师上午试题分析与解答

**试题（1）**

位于 CPU 与主存之间的高速缓冲存储器（Cache）用于存放部分主存数据的拷贝，主存地址与 Cache 地址之间的转换工作由__（1）__完成。

（1）A. 硬件　　B. 软件　　C. 用户　　D. 程序员

**试题（1）分析**

本题考查高速缓冲存储器（Cache）的工作特点。

提供“高速缓存”的目的是为了让数据存取的速度适应 CPU 的处理速度，其基于的原理是内存中“程序执行与数据访问的局域性行为”，即一定程序执行时间和空间内，被访问的代码集中于一部分。为了充分发挥高速缓存的作用，不仅依靠“暂存刚刚访问过的数据”，还要使用硬件实现的指令预测与数据预取技术，即尽可能把将要使用的数据预先从内存中取到高速缓存中。

一般而言，主存使用DRAM技术，而 Cache 使用昂贵但较快速的SRAM技术。

目前微计算机上使用的AMD或Intel微处理器都在芯片内部集成了大小不等的数据高速缓存和指令高速缓存，通称为 L1 高速缓存（L1 Cache，即第一级片上高速缓冲存储器）；而比 L1 容量更大的 L2 高速缓存曾经被放在 CPU 外部（主板或者 CPU 接口卡上），但是现在已经成为 CPU 内部的标准组件；更昂贵的顶级家用和工作站CPU 甚至会配备比 L2 高速缓存还要大的 L3 高速缓存。

**参考答案**

（1）A

**试题（2）**

内存单元按字节编址，地址 0000A000H～0000BFFFH 共有__（2）__个存储单元。

（2）A. 8192k　　B. 1024k　　C. 13k　　D. 8k

**试题（2）分析**

本题考查存储器的地址计算知识。

每个地址编号为一个存储单元(容量为 1 个字节)，地址区间 0000A000H～0000BFFFH 共有 1FFF+1 个地址编号（即 $2^{13}$），1k=1024，因此该地址区间的存储单元数为也就是 8K。

**参考答案**

（2）D

**试题（3）**

相联存储器按__（3）__访问。

（3）A. 地址　　B. 先入后出的方式
　　C. 内容　　D. 先入先出的方式

**试题（3）分析**

本题考查相联存储器的概念。

相联存储器是一种按内容访问的存储器。其工作原理就是把数据或数据的某一部分作为关键字，将该关键字与存储器中的每一单元进行比较，找出存储器中所有与关键字相同的数据字。

相联存储器可用在高速缓冲存储器中，在虚拟存储器中用来作段表、页表或快表存储器，还常用在数据库和知识库中。

**参考答案**

（3）C

**试题（4）**

若 CPU 要执行的指令为：MOV　R1，#45（即将数值 45 传送到寄存器 R1 中），则该指令中采用的寻址方式为__（4）__。

（4）A. 直接寻址和立即寻址　　B. 寄存器寻址和立即寻址
　　C. 相对寻址和直接寻址　　D. 寄存器间接寻址和直接寻址

**试题（4）分析**

本题考查指令系统基础知识。

指令中的寻址方式就是如何对指令中的地址字段进行解释，以获得操作数的方法或获得程序转移地址的方法。常用的寻址方式有：

- 立即寻址。操作数就包含在指令中。
- 直接寻址。操作数存放在内存单元中，指令中直接给出操作数所在存储单元的地址。
- 寄存器寻址。操作数存放在某一寄存器中，指令中给出存放操作数的寄存器名。
- 寄存器间接寻址。操作数存放在内存单元中，操作数所在存储单元的地址在某个寄存器中。
- 间接寻址。指令中给出操作数地址的地址。
- 相对寻址。指令地址码给出的是一个偏移量（可正可负），操作数地址等于本条指令的地址加上该偏移量。
- 变址寻址。操作数地址等于变址寄存器的内容加偏移量。

题目给出的指令中，R1 是寄存器，属于寄存器寻址方式，45 是立即数，属于立即寻址方式。

**参考答案**

（4）B

**试题（5）**

数据流图（DFD）对系统的功能和功能之间的数据流进行建模，其中顶层数据流图描述了系统的__（5）__。

（5）A. 处理过程　　B. 输入与输出
　　C. 数据存储　　D. 数据实体

**试题（5）分析**

本题考查数据流图的基本概念。

数据流图从数据传递和加工的角度，以图形的方式刻画数据流从输入到输出的移动变换过程，其基础是功能分解。对于复杂一些的实际问题，在数据流图中常常出现许多加工，这样看起来不直观，也不易理解，因此用分层的数据流图来建模。按照系统的层次结构进行逐步分解，并以分层的数据流图反映这种结构关系。

在分层的数据流图中，各层数据流图之间应保持"平衡"关系，即输入和输出数据流在各层应该是一致的。

**参考答案**

（5）B

**试题（6）**

以下关于类继承的说法中，错误的是__（6）__。

（6）A. 通过类继承，在程序中可以复用基类的代码
　　B. 在继承类中可以增加新代码
　　C. 在继承类中不能定义与被继承类（基类）中的方法同名的方法
　　D. 在继承类中可以覆盖被继承类（基类）中的方法

**试题（6）分析**

本题考查面向对象的基本知识。

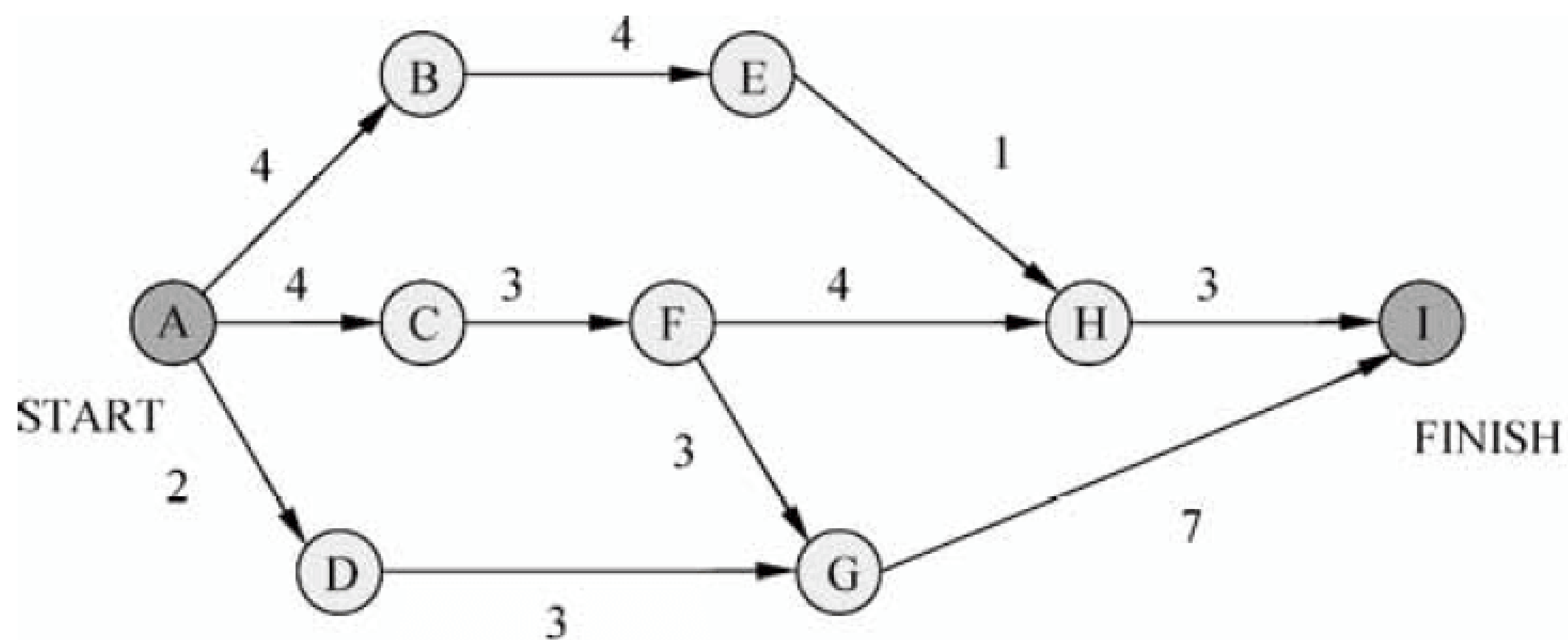
继承是面向对象技术的核心概念之一，它是父类和子类之间共享数据和方法的机制，是类之间的一种关系。在定义和实现一个类的时候，可以在一个已经存在的类的基础上来进行，把这个已经存在的类所定义的内容作为自己的内容，并加入若干新的内容，也可以定义和被继承类相同方法名称的方法，构成方法的重载或覆盖。

**参考答案**

（6）C

**试题（7）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边上的值表示完成活动所需要的时间，则__（7）__在关键路径上。




（7）A. B　　B. C　　C. D　　D. H

**试题（7）分析**

本题考查项目管理及工具技术。

根据关键路径法，计算出关键路径为A→C→F→G→I，关键路径长度为 17。因此里程碑 C 在关键路径上，而里程碑 B、D 和 H 不在关键路径上。

**参考答案**

（7）B

**试题（8）**

软件开发的增量模型＿（8）＿。

（8）A. 最适用于需求被清晰定义的情况

B. 是一种能够快速构造可运行产品的好方法

C. 最适合于大规模团队开发的项目

D. 是一种不适用于商业产品的创新模型

**试题（8）分析**

本题考查软件开发过程模型。增量模型是一种阶段化的软件开发过程模型。在该过程模型中，客户提出系统需求，并指出哪些需求是最重要的。开发团队把软件产品作为一系列的增量构件来设计、编码、集成和测试。每个构件由多个相互作用的模块构成，并且能完成特定的功能。其优点包括：能在较短时间内向用户提交可完成一些有用的工作产品；逐步增加产品的功能，使用户有较充裕的时间学习和适应新产品；项目失败的风险较低；优先级最高的服务首先交付，然后依次将其他构件集成进来，这意味着最重要的服务将接受最多的测试。因此增量模式是一种能够快速构造可运行产品的方法，也适用于今天竞争激烈，需要快速发布产品的市场环境。

**参考答案**

（8）B

**试题（9）**

假设某软件公司与客户签订合同开发一个软件系统，系统的功能有较清晰的定义，且客户对交付时间有严格要求，则该系统的开发最适宜采用＿（9）＿。

（9）A. 瀑布模型 B. 原型模型 C. V 模型 D. 螺旋模型

**试题（9）分析**

本题考查软件过程模型。软件过程是软件生存周期中的一系列相关活动，即用于开发和维护软件及相关产品的一系列活动。瀑布模型从一种非常高层的角度描述了软件开发过程中进行的活动，并且提出了要求开发人员经过的事件序列。该模型适用于项目开始时需求已确定的情况。V 模型是瀑布模型的变种，它说明测试活动是如何与分析和设计相联系的。原型模型允许开发人员快速地构造整个系统或系统的一部分以理解或澄清问题。原型的用途是获知用户的真正需求，因此原型模型可以有效地引发系统需求。螺旋模型把开发活动和风险管理结合起来，以将风险减到最小并控制风险。本题中系统功能有较清晰定义意味着需求较确定，且对交付时间有严格要求，因此最适宜用瀑布模型。

**参考答案**

（9）A

**试题（10）**

中国企业 M 与美国公司 L 进行技术合作，合同约定 M 使用一项在有效期内的美国专利，但该项美国专利未在中国和其他国家提出申请。对于 M 销售依照该专利生产的产品，以下叙述正确的是 （10） 。

（10）A. 在中国销售，M 需要向 L 支付专利许可使用费

B. 返销美国，M 不需要向 L 支付专利许可使用费

C. 在其他国家销售，M 需要向 L 支付专利许可使用费

D. 在中国销售，M 不需要向 L 支付专利许可使用费

**试题（10）分析**

本题考查知识产权知识，涉及专利权的相关概念。知识产权受地域限制，只有在一定地域内知识产权才具有独占性。也就是说，各国依照其本国法律授予的知识产权，只能在其本国领域内受其法律保护，而其他国家对这种权利没有保护的义务，任何人均可在自己的国家内自由使用外国人的知识产品，既无需取得权利人的同意（授权），也不必向权利人支付报酬。例如，中国专利局授予的专利权或中国商标局核准的商标专用权，只能在中国领域内受保护，在其他国家则不给予保护。外国人在我国领域外使用中国专利局授权的发明专利不侵犯我国专利权，如美国人在美国使用我国专利局授权的发明专利不侵犯我国专利权。

通过缔结有关知识产权的国际公约或双边互惠协定的形式，某一国家的国民（自然人或法人）的知识产权在其他国家（缔约国）也能取得权益。参加知识产权国际公约的国家（或者签订双边互惠协定的国家）会相互给予成员国国民的知识产权保护。所以，我国公民、法人完成的发明创造要想在外国受保护，必须在外国申请专利。商标要想在外国受保护，必须在外国申请商标注册。著作权虽然自动产生，但它受地域限制，我国法律对外国人的作品并不是都给予保护，只保护共同参加国际条约国家的公民作品。同

样，参加公约的其他成员国也按照公约规定，对我国公民和法人的作品给予保护。虽然众多知识产权国际条约等的订立使地域性有时会变得模糊，但地域性的特征不但是知识产权最“古老”的特征，也是最基础的特征之一。目前知识产权的地域性仍然存在，是否授予权利、如何保护权利仍须由各缔约国按照其国内法来决定。

本题涉及的依照该专利生产的产品在中国或其他国家销售，中国 M 企业不需要向美国 L 公司支付这件美国专利的许可使用费。这是因为 L 公司未在中国及其他国家申请该专利，不受中国及其他国家专利法的保护，因此依照该专利生产的产品在中国及其他国家销售，M 企业不需要向 L 公司支付这件专利的许可使用费。如果返销美国，需要向 L 公司支付这件专利的许可使用费。这是因为这件专利已在美国获得批准，因而受到美国专利法的保护，M 企业依照该专利生产的产品要在美国销售，则需要向 L 公司支付这件专利的许可使用费。

**参考答案**

（10）D

**试题（11）**

网络中存在各种交换设备，下面的说法中错误的是＿（11）＿。

（11）A. 以太网交换机根据 MAC 地址进行交换

B. 帧中继交换机只能根据虚电路号 DLCI 进行交换

C. 三层交换机只能根据第三层协议进行交换

D. ATM 交换机根据虚电路标识进行信元交换

**试题（11）分析**

以太网交换机根据数据链路层 MAC 地址进行帧交换；帧中继网和 ATM 网都是面向连接的通信网，交换机根据预先建立的虚电路标识进行交换。帧中继的虚电路号是 DLCI，进行交换的协议数据单元为“帧”；而 ATM 网的虚电路号为 VPI 和 VCI，进行交换的协议数据单元为“信元”。

三层交换机是指因特网中使用的高档交换机，这种设备把 MAC 交换的高带宽和低延迟优势与网络层分组路由技术结合起来，其工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住目标 MAC 地址和源 MAC 地址，以及其他相关信息，当再次收到目标地址和源地址相同的帧时就直接进行交换了，不再调用路由功能。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

**参考答案**

（11）C

**试题（12）**

通过以太网交换机连接的一组工作站＿（12）＿。

（12）A. 组成一个冲突域，但不是一个广播域

B. 组成一个广播域，但不是一个冲突域
C. 既是一个冲突域，又是一个广播域
D. 既不是冲突域，也不是广播域

**试题（12）分析**

在网络互联设备中，集线器（Hub）工作于第二层，它把从一个端口接收的数据包分发到其他所有端口。任何时刻集线器只允许一个端口发送数据，所以其连接的各个设备构成一个冲突域，同时也是一个广播域。以太网交换机可以识别数据帧中的地址字段，根据目标地址进行转发，所以这种设备可以允许多个端口同时接收数据。可以说，以太网交换机的所有端口不是一个冲突域，而是一个广播域。

**参考答案**

（12）B

**试题（13）、（14）**

E1 载波的数据速率是__（13）__Mb/s，T1 载波的数据速率是__（14）__Mb/s。

（13）A. 1.544　　B. 2.048　　C. 6.312　　D. 8.448
（14）A. 1.544　　B. 2.048　　C. 6.312　　D. 8.448

**试题（13）、（14）分析**

E1 载波的数据速率是 2.048Mb/s，T1 载波的数据速率是 1.544Mb/s。

**参考答案**

（13）B　（14）A

**试题（15）**

设信道带宽为 3400Hz，采用 PCM 编码，采样周期为125μs，每个样本量化为256 个等级，则信道的数据速率为__（15）__。

（15）A. 10kb/s　　B. 16kb/s　　C. 56kb/s　　D. 64kb/s

**试题（15）分析**

采用 PCM 编码，数据速率与采样周期和量化等级有关。根据题意，每秒采样 8000 次，每个样本提供 8 位数据，所以数据速率 R=8×8000＝64kb/s。考虑到信道带宽为 3400Hz，根据理论分析（奈奎斯特定理和香农定理）和实际情况（有关国际标准），这样的信道是可以提供这个数据速率的。

**参考答案**

（15）D

**试题（16）、（17）**

曼彻斯特编码的效率是__（16）__%，4B/5B 编码的效率是__（17）__%。

（16）A. 40　　B. 50　　C. 80　　D. 100
（17）A. 40　　B. 50　　C. 80　　D. 100

**试题（16）、（17）分析**

在曼彻斯特编码和差分曼彻斯特编码中，每位中间都有一次电平跳变，因此波特率是数据速率的两倍，编码效率为 50%。对于高速网络，如果采用这种编码方法，就需要很高的波特率，其硬件成本则大幅度提高。

为了提高编码的效率，降低电路成本，可以采用 4B/5B 编码。这种编码方法的原理表示如下图所示。




这实际上是一种两级编码方案。在传输介质上传送的是“见 1 就翻不归零码”（NRZ-I），这种编码的效率是 100%，即一个脉冲代表一位。NRZ-I 代码序列中“1”的个数越多，越能提供同步定时信息，但如果遇到长串的“0”，则不能提供同步信息，所以在此之前还需经过一次 4B/5B 编码转换。发送器扫描要发送的位序列，4 位分为一组，然后按照下表的对应规则变换成 5 位的代码。

**4B/5B 编码规则表**

| 十六进制数 | 4 位二进制数 | 4B/5B 码 | 十六进制数 | 4 位二进制数 | 4B/5B 码 |
|---|---|---|---|---|---|
| 0 | 0000 | 11110 | 8 | 1000 | 10010 |
| 1 | 0001 | 01001 | 9 | 1001 | 10011 |
| 2 | 0010 | 10100 | A | 1010 | 10110 |
| 3 | 0011 | 10101 | B | 1011 | 10111 |
| 4 | 0100 | 01010 | C | 1100 | 11010 |
| 5 | 0101 | 01011 | D | 1101 | 11011 |
| 6 | 0110 | 01110 | E | 1110 | 11100 |
| 7 | 0111 | 01111 | F | 1111 | 11101 |

5 位二进制代码共有 32 种状态，在 4B/5B 编码规则表中选用的 5 位代码中 1 的个数都不小于 2 个，这就保证了在介质上传输的代码能提供足够多的同步信息。由于 5 个位实际上表示的是 4 位原始数据，因此其编码效率为 80%。

另外还有 5B/6B、8B/10B 等编码方法，其原理是类似的。

**参考答案**

（16）B　（17）C

**试题（18）～（20）**

ARP 协议的作用是 （18） ，它的协议数据单元封装在 （19） 中传送。ARP 请求是采用 （20） 方式发送的。

（18）A．由 MAC 地址求 IP 地址　　B．由 IP 地址求 MAC 地址

C．由 IP 地址查域名　　D．由域名查 IP 地址

（19）A．IP 分组　　B．以太帧

C．TCP 段　　D．UDP 报文

（20）A．单播　　B．组播

C．广播　　D．点播

**试题（18）～（20）分析**

IP 地址是分配给主机的逻辑地址，在因特网中表示唯一的主机。另外，各个局域网（称为子网）中的主机都有一个子网内部唯一的地址，这种地址是在子网建立时一次性指定的，甚至可能是与网络硬件相关的，称这个地址为主机的物理地址或硬件地址。

从网络互连的角度看，逻辑地址在整个互连网络中有效，而物理地址只是在子网内部有效；逻辑地址由 Internet 层使用，而物理地址由子网访问子层（即数据链路层）使用。

由于有两种主机地址，因而需要一种映像关系能把这两种地址对应起来。在 Internet 中用地址分解协议（Address Resolution Protocol，ARP）来实现逻辑地址到物理地址映像。ARP 分组的格式如下图所示，各字段的含义解释如下：

- 硬件类型：网络接口硬件的类型，对以太网此值为 1。
- 协议类型：发送方使用的协议，0800H 表示 IP 协议。
- 硬件地址长度：对以太网，地址长度为 6 字节。
- 协议地址长度：对 IP 协议，地址长度为 4 字节。
- 操作类型：
  - 1——ARP 请求；
  - 2——ARP 响应；
  - 3——RARP 请求；
  - 4——RARP 响应。

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td>操作类型</td></tr>
<tr><td colspan="3">发送结点硬件地址</td></tr>
<tr><td colspan="3">发送结点协议地址</td></tr>
<tr><td colspan="3">目标结点硬件地址</td></tr>
<tr><td colspan="3">目标结点协议地址</td></tr>
</table>

通常 Internet 应用程序把要发送的报文交给 IP 协议，IP 当然知道接收方的逻辑地址

（否则就不能通信了），但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路实体之前可以用两种方法得到目标物理地址：

（1）查本地内存中的 ARP 地址映像表，其逻辑结构如下表所示。可以看出这是 IP 地址和以太网地址的对照表。

（2）如果 ARP 表查不到，就广播一个 ARP 请求分组，这种分组经过路由器进一步转发，可以到达所有连网的主机。收到该分组的主机一方面可以用分组中的两个源地址更新自己的 ARP 地址映像表，一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址；若不相符，则不予回答。

**ARP 地址映像表**

| IP 地址 | 以太网地址 |
|---|---|
| 130.130.87.1 | 08 00 39 00 29 D4 |
| 129.129.52.3 | 08 00 5A 21 17 22 |
| 192.192.30.5 | 08 00 10 99 A1 44 |

**参考答案**

（18）B （19）B （20）C

**试题（21）～（23）**

RIP 是一种基于__（21）__算法的路由协议，一个通路上最大跳数是__（22）__，更新路由表的原则是到各个目标网络的__（23）__。

（21）A. 链路状态 B. 距离矢量 C. 固定路由 D. 集中式路由

（22）A. 7 B. 15 C. 31 D. 255

（23）A. 距离最短 B. 时延最小 C. 流量最小 D. 路径最空闲

**试题（21）～（23）分析**

RIP 协议采用 Bellman-Ford 的距离矢量路由算法，用于在 TCP/IP 的网络中计算最佳路由。RIP 以跳步计数（hop count）来度量路由费用，跳步数最小被认为是距离最短。RIP 适用于小型网络，允许的跳步数不超过 15 跳，16 跳是不可到达网络，经过 16 跳的任何分组将被路由器丢弃。

**参考答案**

（21）B （22）B （23）A

**试题（24）、（25）**

OSPF 协议使用__（24）__报文来保持与其邻居的连接。下面关于 OSPF 拓扑数据库的描述中，正确的是__（25）__。

（24）A. Hello B. Keepalive C. SPF D. LSU

（25）A. 每一个路由器都包含了拓扑数据库的所有选项

B. 在同一区域中的所有路由器包含同样的拓扑数据库

C. 使用 Dijkstra 算法来生成拓扑数据库

D. 使用 LSA 分组来更新和维护拓扑数据库

**试题（24）、（25）分析**

OSPF 是一种链路状态协议，用于在自治系统内部的路由器之间交换路由信息。OSPF 路由器根据收集到的链路状态信息构造网络拓扑结构图，使用Dijkstra 最短通路优先算法（SPF）计算到达各个目标的最佳路由。

下表列出了 OSPF 协议的 5 种报文，这些报文通过 TCP 连接传送。OSPF 路由器启动后以固定的时间间隔泛洪传播Hello 报文，采用目标地址224.0.0.5 代表所有的 OSPF 路由器。在点对点网络上每 10s 发送一次，在 NBMA 网络中每 30s 发送一次。管理 Hello 报文交换的规则称为 Hello 协议。Hello 协议用于发现邻居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

**OSPF 的 5 种报文类型表**

| 类型 | 报 文 类 型 | 功 能 描 述 |
|---|---|---|
| 1 | Hello | 用于发现相邻的路由器 |
| 2 | 数据库描述 DBD（DataBase Description） | 表示发送者的链路状态数据库内容 |
| 3 | 链路状态请求 LSR（Link-State Request） | 向对方请求链路状态信息 |
| 4 | 链路状态更新 LSU（Link-State Update） | 向邻居路由器发送链路状态通告 |
| 5 | 链路状态应答 LSAck（Link-State Acknowledgement） | 对链路状态更新报文的应答 |

OSPF 路由器之间通过链路状态公告（Link State Advertisment，LSA）交换网络拓扑信息。LSA 中包含连接的接口、链路的度量值（Metric）等信息。

在多区域网络中，OSPF 路由器可以按不同的功能划分为以下 4 种：

① 内部路由器。所有接口在同一区域内的路由器，只维护一个链路状态数据库。

② 主干路由器。具有连接主干区域接口的路由器。

③ 区域边界路由器（ABR）。连接多个区域的路由器，一般作为一个区域的出口。ABR 为每一个连接的区域建立一个链路状态数据库，负责将所连接区域的路由摘要信息发送到主干区域，而主干区域上的 ABR 则负责将这些信息发送给各个区域。

④ 自治系统边界路由器（ASBR）。至少拥有一个连接外部自治系统接口的路由器，负责将外部非 OSPF 网络的路由信息传入 OSPF 网络。

在正常情况下，区域内的路由器与本区域的 DR 和 BDR 通过互相发送数据库描述报文（DBD）交换链路状态信息。路由器把收到的链路状态信息与自己的链路状态数据库进行比较，如果发现接收到了不在本地数据库中的链路信息，则向其邻居发送链路状态请求报文 LSR，要求传送有关该链路的完整更新信息。接收到 LSR 的路由器用链路状态更新 LSU 报文响应，其中包含了有关的链路状态通告 LSA。LSAck 用于对 LSU 进行

确认。

根据以上说明，并不是每个路由器都包含了拓扑数据库的所有选项，在同一区域中的路由器包含的拓扑数据库也不一定完全相同。

**参考答案**

（24）A （25）D

**试题（26）、（27）**

TCP 协议使用__（26）__次握手机制建立连接，当请求方发出 SYN 连接请求后，等待对方回答__（27）__，这样可以防止建立错误的连接。

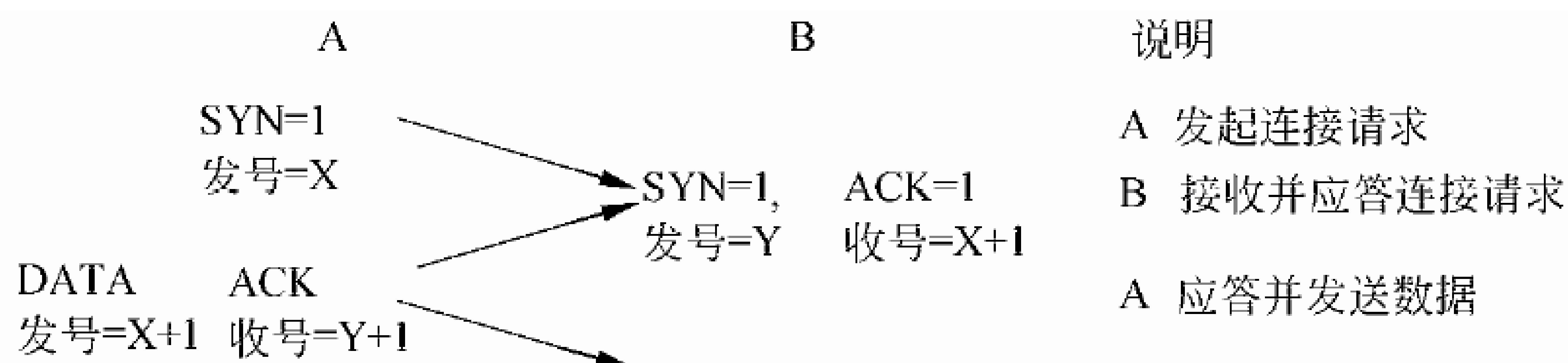
（26）A．1 B．2 C．3 D．4

（27）A．SYN,ACK B．FIN,ACK C．PSH,ACK D．RST,ACK

**试题（26）、（27）分析**

TCP 建立和释放连接的过程采用三次握手协议。这种协议的目的是连接两端都要声明自己的连接端点标识，并回答对方的连接端点标识，以确保不出现错误的连接。

同步标志 SYN 用于连接建立阶段。建立连接的过程如下：首先是发起方发送一个 SYN 标志置位的段，其中的发送顺序号为某个值 X，称为初始顺序号（Initial Sequence Number，ISN），接收方以 SYN 和 ACK 标志置位的段响应，其中的应答顺序号应为 X+1（表示期望从第 X+1 个字节处开始接收数据），发送顺序号为某个值 Y（接收端指定的 ISN）。这个段到达发起端后，发起端以 ACK 标志置位，应答顺序号为 Y+1 的段回答，连接就正式建立了。可见，所谓初始顺序号是收发双方对连接的标识，也与字节流的位置有关，参见下图。




**参考答案**

（26）C （27）A

**试题（28）、（29）**

采用 DHCP 分配 IP 地址无法做到__（28）__，当客户机发送 dhcpdiscover 报文时采用__（29）__方式发送。

（28）A．合理分配 IP 地址资源 B．减少网管员工作量

C．减少 IP 地址分配出错可能 D．提高域名解析速度

（29）A．广播 B．任意播 C．组播 D．单播

**试题（28）、（29）分析**

本题考查考生对 DHCP 协议及其工作过程的掌握程度。采用 DHCP 协议可以自动分配 IP 地址，便于网络管理员依据上网实际用户数合理、动态地分配地址资源，从而达到减轻工作量的目的。由于 IP 地址资源的分配是由服务器依据地址池进行分配的，减少了分配地址出错的可能，但地址的分配和域名解析不存在直接的联系，无法做到提高域名解析速度。

通过 DHCP 服务器分配 IP 地址的工作流程为：寻找 DHCP 服务器、提供 IP 租用、接受 IP 租约及租约确认 4 步，分别对应的报文为 Dhcpdiscover、Dhcpoffer、Dhcprequest 和 Dhcpack。当客户端发送 dhcpdiscover 报文时尚不清楚提供服务的 DHCP 服务器，只能采用广播方式发送。

**参考答案**

（28）D　（29）A

**试题（30）**

客户端登录 FTP 服务器后使用__（30）__命令来上传文件。

（30）A．get　　B．!dir　　C．put　　D．bye

**试题（30）分析**

本题考查 FTP 服务器相关命令。部分命令及功能如下：

- put：put 或 send 的功能是把本地计算机的一个文件上传到远程主机上。
- get：get 或 recv 的功能是下载远程主机的一个文件到自己的计算机上。
- !dir：显示远程计算机上的目录文件和子目录列表。
- bye：结束 FTP 服务。

**参考答案**

（30）C

**试题（31）**

SMTP 传输的邮件报文采用__（31）__格式表示。

（31）A．ASCII　　B．ZIP　　C．PNP　　D．HTML

**试题（31）分析**

本题考查 SMTP 协议及相关服务。SMTP 传输的邮件报文需采用 ASCII 进行编码。

**参考答案**

（31）A

**试题（32）**

在下列选项中，属于 IIS 6.0 提供的服务组件是__（32）__。

（32）A. Samba　　B. FTP　　C. DHCP　　D. DNS

**试题（32）分析**

本题考查 IIS6.0 组件及相关服务。IIS 6.0 提供了更为方便的安装/管理功能和增强的

应用环境、基于标准的分布协议、改进的性能表现和扩展性，以及更好的稳定性和易用性。其服务组件包括：

① WWW服务。WWW是图形最为丰富的Internet服务。Web具有很强的链接能力，支持协作和工作流程，可以给分布在世界各地的用户提供商业应用程序。

② FTP服务。文件传输协议是在Internet中两个远程计算机之间传送文件的协议。该协议允许用户使用FTP命令对远程计算机中的文件系统进行操作。

③ SMTP服务。简单邮件传输协议在客户端应用程序和远程计算机的邮件服务器之间传送邮件信息。

④ POP3服务。POP3的功能是邮件的存储和管理，能为用户提供账号、密码和身份验证功能，与SMTP服务配合，提供完整的邮件服务。

**参考答案**

（32）B

**试题（33）**

与route print具有相同功能的命令是（33）。

（33）A．ping　　B．arp -a　　C．netstat -r　　D．tracert -d

**试题（33）分析**

本题考查网络管理命令的使用及其作用。

route print用于显示路由表项，比如要显示整个路由器的内容，则输入“route print”；要显示路由表中以“10.”开头的表项，则输入“route print 10.*”。

Netstat命令用于显示TCP连接、计算机正在监听的端口、以太网统计信息、IP路由表、IPv4统计信息（包括IP、ICMP、TCP和UDP等协议）和IPv6统计信息（包括IPv6、ICMPv6、TCP over IPv6和UDP over IPv6等协议）等。Netstat -r显示IP路由表的内容，其作用等价于路由打印命令route print。

**参考答案**

（33）C

**试题（34）**

下面的Linux命令中，能关闭系统的命令是（34）。

（34）A．kill　　B．shutdown　　C．exit　　D．logout

**试题（34）分析**

本题考查Linux基本操作方面的知识。

题中的4个选项中，kill用于发送SIGKILL信号，可以用于杀死进程；shutdown用于关闭系统；exit是一个系统调用，用于退出进程，也是一个命令，可以关闭控制台程序；logout用于注销用户。

**参考答案**

（34）B

**试题（35）**

在 Linux 中，DNS 服务器的配置文件是（35）。

（35）A. /etc/hostname　B. /etc/host.conf
C. /etc/resolv.conf　D. /etc/httpd.conf

**试题（35）分析**

本题考查 DNS 服务器配置方面的知识。

DNS 服务器的配置文件是/etc/resolv.conf，Web 服务器的配置文件是/etc/httpd.conf。

**参考答案**

（35）C

**试题（36）**

在 Linux 中，可以利用（36）命令来终止某个进程。

（36）A. kill　B. dead　C. quit　D. exit

**试题（36）分析**

本题考查 Linux 基本操作方面的知识。

kill 可以用于终止进程；dead 不是一个有效命令；quit 和 exit 可以用于关闭控制台程序。

**参考答案**

（36）A

**试题（37）**

DNS 服务器中提供了多种资源记录，其中（37）定义了区域的邮件服务器及其优先级。

（37）A. SOA　B. NS　C. PTR　D. MX

**试题（37）分析**

本题考查 DNS 服务器中提供的资源记录。

资源记录分为许多不同的类型，常用的有：

- SOA（Start Of Authoritative）：开始授权记录是区域文件的第一条记录，指明区域的主服务器，指明区域管理员的邮件地址，并给出区域复制的有关信息。
- 生命期（TTL）：资源记录在其他名字服务器缓存中保存的最少有效时间（秒）。
- A（Address）：地址记录表示主机名到 IP 地址的映像。
- PTR（Pointer）：指针记录是 IP 地址到主机名的映射。
- NS（Name Server）：给出区域的授权服务器。
- MX（Mail eXchanger）：定义了区域的邮件服务器及其优先级（搜索顺序）。
- CNAME：为正式主机名（canonical name）定义了一个别名（alias）。

**参考答案**

（37）D

**试题（38）、（39）**

某用户正在 Internet 浏览网页，在 Windows 命令窗口中输入__（38）__命令后得到下图所示的结果。

```
C:\Documents and Settings\User>
Interface: 219.245.67.192 --- 0x2
 Internet Address      Physical Address     Type
 219.245.67.254       10-2B-89-2A-16-7D    dynamic
```

若采用抓包器抓获某一报文的以太帧如下图所示，该报文是__（39）__。

```
0000  00 23 89 1a 06 7c 00 1d  7d 39 62 3e 08 00 45 00   .#...|.. }9b>..E.
0010  01 ed 48 94 40 00 40 06  7f 28 db f5 43 c0 77 4b   ..H.@.@. .(..C.wK
0020  da 4d 0d e0 00 50 59 90  15 ef 20 c1 07 84 50 18   .M...PY. .. ...P.
0030  ff ff 73 2e 00 00 47 45  54 20 2f 20 48 54 54 50   ..s...GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 69 6d   /1.1..Ac cept: im
0050  61 67 65 2f 67 69 66 2c  20 69 6d 61 67 65 2f 78   age/gif,  image/x
0060  2d 78 62 69 74 6d 61 70  2c 20 69 6d 61 67 65 2f   -xbitmap , image/
0070  6a 70 65 67 2c 20 69 6d  61 67 65 2f 70 6a 70 65   jpeg, im age/pjpe
0080  67 2c 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   g, appli cation/x
0090  2d 73 68 6f 63 6b 77 61  76 65 2d 66 6c 61 73 68   -shockwa ve-flash
00a0  2c 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6d 73   , applic ation/ms
00b0  77 6f 72 64 2c 20 61 70  70 6c 69 63 61 74 69 6f   word, ap plicatio
```

（38）A． arp-a　　B． ipconfig /all　　C． route　　D. nslookup

（39）A． 由本机发出的 Web 页面请求报文

B． 由 Internet 返回的 Web 响应报文

C． 由本机发出的查找网关 MAC 地址的 ARP 报文

D． 由 Internet 返回的 ARP 响应报文

**试题（38）、（39）分析**

本题考查对实际的网络管理与分析工具的使用情况。

图中显示的是 IP 地址与物理地址的映射表，实现这一功能的协议是 ARP，命令为 arp-a。

从结果图中可以从两个方面得出报文的信息：首先从图中右侧的文字信息 GET 和 HTTP 1.0 中可以看出，是由客户端发送的 HTTP 请求报文，因此是由本机发出的Web 页面请求报文。此外，从捕获的以太帧中，目的 MAC 为网关、源 IP 为本地 PC 也能判断出相同结果。

**参考答案**

（38）A　（39）A

**试题（40）**

在 Windows 系统中，默认权限最低的用户组是__（40）__。

（40）A. everyone　　B. administrators　　C. power users　　D. users

**试题（40）分析**

本题考查 Windows 用户权限方面的知识。

在以上 4 个选项中，用户组默认权限由高到低的顺序是 administrators→power users→users→everyone。

**参考答案**

（40）A

**试题（41）**

IIS 6.0 支持的身份验证安全机制有 4 种验证方法， 其中安全级别最高的验证方法是<u>（41）</u>。

（41）A. 匿名身份验证　　　　B. 集成 Windows 身份验证
C. 基本身份验证　　　　D. 摘要式身份验证

**试题（41）分析**

本题考查 Windows IIS 服务中身份认证的基础知识。

Windows IIS 服务支持的身份认证方式有.NET Passport 身份验证、集成 Windows 身份验证、摘要式身份验证和基本身份验证。

① 集成 Windows 身份验证：以 Kerberos 票证的形式通过网络向用户发送身份验证信息，并提供较高的安全级别。Windows 集成身份验证使用 Kerberos 版本 5 和 NTLM 身份验证。

② 摘要式身份验证：将用户凭据作为 MD5 哈希或消息摘要在网络中进行传输，这样就无法根据哈希对原始用户名和密码进行解码。

③ .NET Passport 身份验证：对 IIS 的请求必须在查询字符串或 Cookie 中包含有效的.NET Passport 凭据，提供了单一登录安全性，为用户提供对 Internet 上各种服务的访问权限。

④ 基本身份验证：用户凭据以明文形式在网络中发送。这种形式提供的安全级别很低，因为几乎所有协议分析程序都能读取密码。

**参考答案**

（41）B

**试题（42）**

以下关于钓鱼网站的说法中，错误的是<u>（42）</u>。

（42）A. 钓鱼网站仿冒真实网站的 URL 地址
B. 钓鱼网站是一种网络游戏
C. 钓鱼网站用于窃取访问者的机密信息
D. 钓鱼网站可以通过 Email 传播网址

**试题（42）分析**

本题考查网络安全方面的知识。

钓鱼网站是指一类仿冒真实网站的 URL 地址，通过 E-mail 传播网址，目的是窃取用户账号、密码等机密信息的网站。

**参考答案**

（42）B

**试题（43）**

支持安全Web服务的协议是__（43）__。

（43）A. HTTPS　　B. WINS　　C. SOAP　　D. HTTP

**试题（43）分析**

本题考查网络安全方面的知识。

Web服务的标准协议是HTTP协议，HTTPS对HTTP协议增加了一些安全特性。WINS是Windows系统的一种协议。SOAP是基于HTTP和XML，用于Web Service的简单对象访问协议。

**参考答案**

（43）A

**试题（44）**

甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用__（44）__验证该消息的真实性。

（44）A. 甲的公钥　　B. 甲的私钥　　C. 乙的公钥　　D. 乙的私钥

**试题（44）分析**

本题考查数字签名的概念。

数字签名（Digital Signature）技术是不对称加密算法的典型应用：数据源发送方使用自己的私钥对数据校验和（或）其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名主要的功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

**参考答案**

（44）A

**试题（45）**

下列算法中，__（45）__属于摘要算法。

（45）A. DES　　B. MD5　　C. Diffie-Hellman　　D. AES

**试题（45）分析**

本题考查安全算法方面的知识。

题中的4个选项中，DES是一种经典的数据加密算法，AES是高级加密算法，Diffie-Hellman是一种密钥交换算法，MD5和SHA属于报文摘要算法。

**参考答案**

（45）B

**试题（46）**

网络的可用性是指 （46） 。

（46）A. 网络通信能力的大小　　B. 用户用于网络维修的时间
C. 网络的可靠性　　D. 用户可利用网络时间的百分比

**试题（46）分析**

可用性是指网络系统、网络元素或网络应用对用户可利用的时间的百分比。有些应用对可用性很敏感，例如，飞机订票系统若宕机一小时，就可能减少几十万元的票款；而股票交易系统如果中断运行一分钟，就可能造成几千万元的损失。实际上，可用性是网络元素可靠性的表现，而可靠性是指网络元素在具体条件下完成特定功能的概率。如果用平均无故障时间（Mean Time Between Failure，MTBF）来度量网络元素的故障率，则可用性 A 可表示为 MTBF 的函数：

$$A=\frac{MTBF}{MTBF+MTTR}$$

其中，MTTR（Mean Time To Repair）为发生失效后的平均维修时间。由于网络系统由许多网络元素组成，因此系统的可靠性不但与各个元素的可靠性有关，而且还与网络元素的组织形式有关。根据可靠性理论，由元素串并联组成的系统的可用性与网络元素的可用性之间的关系如下图所示。

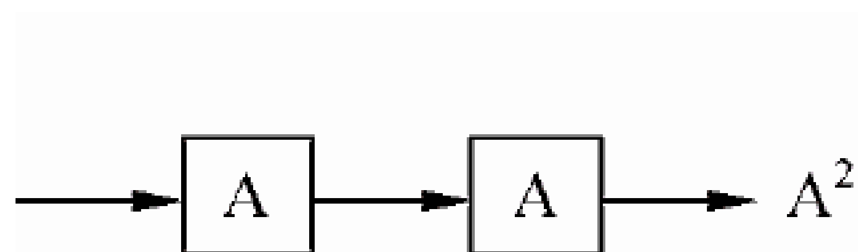


图 a　串联

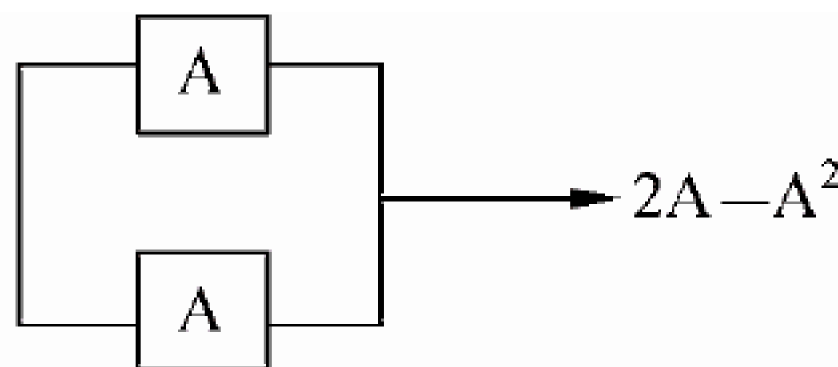


图 b　并联

从图 a 可以看出，若两个元素串联，则可用性减少。例如，两个 Modem 串联在链路的两端，若单个 Modem 的可用性 A=0.98，并假定链路其他部分的可用性为 1，则整个链路的可用性 A=0.98×0.98=0.9604。从图 b 可以看出，若两个元素并联，则可用性增加。例如，终端通过两条链路连接到主机，若一条链路失效，另外一条链路自动备份。假定单个链路的可用性 A=0.98，则双链路的可用性 A=2×0.98－0.98×0.98= 1.96－0.9604=0.9996。

**参考答案**

（46）D

**试题（47）**

网络管理的 5 大功能域是 （47） 。

（47）A. 配置管理、故障管理、计费管理、性能管理和安全管理
B. 配置管理、故障管理、计费管理、带宽管理和安全管理
C. 配置管理、故障管理、成本管理、性能管理和安全管理

D. 配置管理、用户管理、计费管理、性能管理和安全管理

**试题（47）分析**

网络管理有 5 大功能域：故障管理（Fault Management）、配置管理（Configuration Management）、计费管理（Accounting Management）、性能管理（Performance Management）和安全管理（Security Management），简写为 F-CAPS。

**参考答案**

（47）A

**试题（48）**

SNMPv2 提供了 3 种访问管理信息的方法，这 3 种方法不包括__（48）__。

（48）A. 管理站向代理发出通信请求　　B. 代理向管理站发出通信请求
C. 管理站与管理站之间的通信　　D. 代理向管理站发送陷入报文

**试题（48）分析**

SNMPv2 提供了 3 种访问管理信息的方法：

- 管理站和代理之间的请求/响应通信，这种方法与 SNMPv1 是一样的。
- 管理站和管理站之间的请求/响应通信，这种方法是 SNMPv2 特有的，可以由一个管理站把有关管理信息告诉另外一个管理站。
- 代理系统到管理站的非确认通信，即由代理向管理站发送陷入报文，报告出现的异常情况。SNMPv1 中也有对应的通信方式。

**参考答案**

（48）B

**试题（49）**

嗅探器改变了网络接口的工作模式，使得网络接口__（49）__。

（49）A. 只能够响应发送给本地的分组
B. 只能够响应本网段的广播分组
C. 能够响应流经网络接口的所有分组
D. 能够响应所有组播信息

**试题（49）分析**

由于以太网采用广播通信方式，因此在网络中传送的分组可以出现在同一冲突域中的所有端口上。在常规状态下，网卡控制程序只接收发送给自己的数据包和广播包，对目标地址不是自己的数据包则丢弃之。如果把网卡配置成混杂模式（Promiscuous Mode），它就能接收所有分组，无论是否是发送给自己的。

混杂模式通信被广泛地使用在恶意软件中，最初是为了获取根用户权限（Root Compromise），继而进行 ARP 欺骗（ARP Spoofing）。凡是进行 ARP 欺骗的计算机必定把网卡设置成了混杂模式，所以检测那些滥用混杂模式的计算机是很重要的。

嗅探器（Sniffer）就是采用混杂模式工作的协议分析器，可以用纯软件实现，运行

在普通的计算机上，也可以做成硬件，用独立设备实现高效率的网络监控。“Sniffer Network Analyzer”是美国网络联盟公司（Network Associates INC，NAI）的注册商标，然而许多采用类似技术的网络协议分析产品也可以叫作嗅探器。NAI 是电子商务和网络安全解决方案的主要供应商，它的产品除了 Sniffer Pro 之外，还有著名的防毒软件 McAfee。

**参考答案**

（49）C

**试题（50）、（51）**

ICMP 协议的功能包括<u>（50）</u>，当网络通信出现拥塞时，路由器发出 ICMP<u>（51）</u>报文。

（50）A. 传递路由信息　　B. 报告通信故障
　　C. 分配网络地址　　D. 管理用户连接

（51）A. 回声请求　　B. 掩码请求
　　C. 源抑制　　D. 路由重定向

**试题（50）、（51）分析**

ICMP（Internet control Message Protocol）与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送，报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

| 类　型 | 代　码 | 校验和 |
|---|---|---|
| 参　数 | | |
| 信息（可变长） | | |

下面解释常见的 ICMP 报文的含义。

① 目标不可到达（类型 3）：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。

② 超时（类型 11）：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。

③ 源抑制（类型 4）：这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑

制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。

④ 参数问题（类型 12）：如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。

⑤ 路由重定向（类型 5）：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如，路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。

⑥ 回声（请求/响应，类型 8/0）：用于测试两个结点之间的通信线路是否畅通。收到回声请求的结点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。

⑦ 时间戳（请求/响应，类型 13/14）：用于测试两个结点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

⑧ 地址掩码（请求/响应，类型 17/18）：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标结点与源结点是否在同一 LAN 中。

**参考答案**

（50）B （51）C

**试题（52）**

IP 地址分为公网地址和私网地址，以下地址中属于私网地址的是（52）。

（52）A. 10.216.33.124 B. 127.0.0.1 C. 172.34.21.15 D. 192.32.146.23

**试题（52）分析**

私网地址不能在公网上出现，只能用在内部网络中，所有的路由器都不转发目标地址为私网地址的数据报。下面的地址都是私网地址：

- 10.0.0.0～10.255.255.255 1 个 A 类地址
- 172.16.0.0～172.31.255.255 16 个 B 类地址
- 192.168.0.0～192.168.255.255 256 个 C 类地址

**参考答案**

（52）A

**试题（53）**

如果子网 172.6.32.0/20 被划分为子网 172.6.32.0/26，则下面的结论中正确的是（53）。

（53）A. 被划分为 62 个子网　　B. 每个子网有 64 个主机地址
　　C. 被划分为 32 个子网　　D. 每个子网有 62 个主机地址

**试题（53）分析**

子网 172.6.32.0/20 被划分为子网 172.6.32.0/26，网络掩码增加了 6 位，被划分成了 64 个子网，每个子网的主机 ID 部分为 6 位，可以提供主机地址个数为 62。

**参考答案**

（53）D

**试题（54）、（55）**

地址 192.168.37.192/25 是<u>（54）</u>，地址 172.17.17.255/23 是<u>（55）</u>。

（54）A. 网络地址　　B. 组播地址
　　C. 主机地址　　D. 定向广播地址

（55）A. 网络地址　　B. 组播地址
　　C. 主机地址　　D. 定向广播地址

**试题（54）、（55）分析**

地址 192.168.37.192/25 的二进制展开形式为（黑体部分为网络 ID）：

**11000000 10101000 00100101 1**1000000，可见这是一个主机地址。

地址 172.17.17.255/23 的二进制展开形式为（黑体部分为网络 ID）：

**10101100 00010001 0001000**1 11111111，可见这是一个广播地址。

**参考答案**

（54）C　（55）D

**试题（56）、（57）**

某公司有 2000 台主机，则必须给它分配<u>（56）</u>个 C 类网络。为了使该公司的网络地址在路由表中只占一行，给它指定的子网掩码必须是<u>（57）</u>。

（56）A. 2　　B. 8　　C. 16　　D. 24

（57）A. 255.192.0.0　　B. 255.240.0.0
　　C. 255.255.240.0　　D. 255.255.248.0

**试题（56）、（57）分析**

每个 C 类网络可提供 254 个主机地址，2000 台主机大约需要 8 个 C 类网络，这些子网合成一个超网，其网络掩码应为 255.255.248.0。

**参考答案**

（56）B　（57）D

**试题（58）**

以下给出的地址中，属于子网 172.112.15.19/28 的主机地址是<u>（58）</u>。

（58）A. 172.112.15.17　　B. 172.112.15.14
　　C. 172.112.15.16　　D. 172.112.15.31

**试题（58）分析**

子网 172.112.15.19/28 的二进制形式为 **10101100 01110000 00001111 0001**0011。

4 个选项的展开形式分别为：

选项 A：172.112.15.17：10101100 01110000 00001111 00010001

选项 B：172.112.15.14：10101100 01110000 00001111 00001110

选项 C：172.112.15.16：10101100 01110000 00001111 00010000

选项 D：172.112.15.31：10101100 01110000 00001111 00011111

可以看出，选项 A 属于该子网的主机地址，选项 C 是子网地址，而选项 D 是该子网的广播地址。

**参考答案**

（58）A

**试题（59）**

IPv6 地址分为 3 种类型，它们是 （59） 。

（59）A. A 类地址、B 类地址、C 类地址

B. 单播地址、组播地址、任意播地址

C. 单播地址、组播地址、广播地址

D. 公共地址、站点地址、接口地址

**试题（59）分析**

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址有 3 种类型：

① 单播（Unicast）地址。

单播地址是单个网络接口的标识符。对于有多个接口的结点，其中任何一个单播地址都可以用作该结点的标识符。但是为了满足负载平衡的需要，在 RFC 2373 中规定，只要在实现中多个接口看起来形同一个接口就允许这些接口使用同一地址。IPv6 的单播地址是用一定长度的格式前缀汇聚的地址，类似于 IPv4 中的 CIDR 地址。单播地址中有下列两种特殊地址：

- 不确定地址。地址 0:0:0:0:0:0:0:0 称为不确定地址，不能分配给任何结点。不确定地址可以在初始化主机时使用，在主机未取得地址之前，它发送的 IPv6 分组中的源地址字段可以使用这个地址。这种地址不能用作目标地址，也不能用在 IPv6 路由头中。
- 回环地址。地址 0:0:0:0:0:0:0:1 称为回环地址，结点用这种地址向自身发送 IPv6 分组。这种地址不能分配给任何物理接口。

② 任意播（AnyCast）地址。

这种地址表示一组接口（可属于不同结点的）的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对 IPv6 任意播地址存在下列

限制：

- 任意播地址不能用作源地址，而只能作为目标地址。
- 任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

③ 组播（MultiCast）地址。

组播地址是一组接口（一般属于不同结点）的标识符，发往组播地址的分组被传送给该地址标识的所有接口。IPv6 中没有广播地址，它的功能已被组播地址所代替。

在 IPv6 地址中，任何全“0”和全“1”字段都是合法的，除非特别排除的之外。特别是前缀可以包含“0”值字段，也可以用“0”作为终结字段。一个接口可以被赋予任何类型的多个地址（单播、任意播、组播）或地址范围。

**参考答案**

（59）B

**试题（60）**

FTP 默认的控制连接端口是<u>（60）</u>。

（60）A. 20　　B. 21　　C.23　　D. 25

**试题（60）分析**

FTP 默认的控制连接端口是 21，数据连接的端口号是 20。

**参考答案**

（60）B

**试题（61）**

路由器命令“Router(config)# access-list 1 deny 192.168.1.1”的含义是<u>（61）</u>。

（61）A. 不允许源地址为 192.168.1.1 的分组通过
B. 允许源地址为 192.168.1.1 的分组通过
C. 不允许目标地址为 192.168.1.1 的分组通过
D. 允许目标地址为 192.168.1.1 的分组通过

**试题（61）分析**

标准 ACL 语句只能根据数据包中的源地址进行过滤，可以允许（permit）或阻止（deny）数据包通过。配置标准 ACL 的路由器命令格式如下：

```
Router(config)# access-list ACL_#  permit|deny source_IP_address
[wildcard_mask] [log]
```

标准 ACL 的编号为 1～99 和 1300～1999，编号之后是路由器实施的动作。匹配条件仅考虑分组的源地址，后随一个任选的通配符掩码。如果忽略了通配符掩码，则默认为 0.0.0.0，即要求整个地址全部匹配。最后的任选 log 参数使得匹配的分组在路由器控制台端口打印输出，但是不会在远程连接的路由器上输出。

路由器命令“Router(config)# access-list 1 deny 192.168.1.1”的含义是阻止源地址为

192.168.1.1 的分组通过。

**参考答案**

（61）A

**试题（62）**

局域网冲突时槽的计算方法如下。假设 $t_{PHY}$ 表示工作站的物理层时延，C 表示光速，S 表示网段长度，$t_R$ 表示中继器的时延，在局域网最大配置的情况下，冲突时槽等于＿（62）＿。

（62）A. $S/0.7C+2t_{PHY}+8t_R$　　B. $2S/0.7C+2t_{PHY}+8t_R$

C. $2S/0.7C+t_{PHY}+8t_R$　　D. $2S/0.7C+2t_{PHY}+4t_R$

**试题（62）分析**

IEEE 802.3 标准规定的冲突时槽计算方法适用于由 4 个中继器连接的、5 个网段组成的最大配置，整个网络长度达到 2500m，其公式为 $2S/0.7C+2t_{PHY}+8t_R$。其中 2S 表示整个网络长度 2 倍，即来回传输一圈的距离。0.7C 表示光速的 0.7 倍，2S/0.7C 表示来回传输的时延。$2t_{PHY}$ 表示网络两端相距最远的两个网站的物理层时延，而 $8t_R$ 表示来回传输时经过各个中继器的时延。

**参考答案**

（62）B

**试题（63）**

在局域网标准中，100Base-T 规定从收发器到集线器的距离不超过＿（63）＿米。

（63）A. 100　　B. 185　　C. 300　　D. 1000

**试题（63）分析**

在局域网标准中，100Base-T 规定从收发器到集线器的距离不超过 100 米。

**参考答案**

（63）A

**试题（64）**

IEEE 802.11 在 MAC 层采用了＿（64）＿协议。

（64）A. CSMA/CD　　B. CSMA/CA

C. DQDB　　D. 令牌传递

**试题（64）分析**

IEEE 802.11 在 MAC 层采用了 CSMA/CA 协议，即载波监听多路访问/冲突避免协议。其所以不使用 CSMA/CD 是因为在无线传输的情况下会出现隐蔽终端的问题，使得冲突检测不可行。

**参考答案**

（64）B

**试题（65）、（66）**

在无线局域网中，AP 的作用是（65）。新标准 IEEE 802.11n 提供的最高数据速率可达到（66）。

（65）A. 无线接入　B. 用户认证　C. 路由选择　D. 业务管理

（66）A. 54Mb/s　B. 100Mb/s　C. 200Mb/s　D. 300Mb/s

**试题（65）、（66）分析**

在无线局域网中，AP 的作用是无线接入，但通常使用的无线路由器则增加了路由等更加复杂的功能。新标准 IEEE 802.11n 提供的最高数据速率可达到 300Mb/s，这也是目前市售的无线接入设备提供的最高数据速率。

**参考答案**

（65）A　（66）D

**试题（67）**

IEEE 802.16 工作组提出的无线接入系统空中接口标准是（67）。

（67）A. GPRS　B. UMB　C. LTE　D. WiMAX

**试题（67）分析**

IEEE 802.16 工作组提出的无线接入系统空中接口标准是一种无线城域网技术，许多网络运营商都加入了支持这个标准的行列。WiMAX（World Interoperability for Microwave Access）论坛是由 Intel 等芯片制造商于 2001 年发起成立的财团，其任务是对 IEEE 802.16 产品进行一致性认证，促进标准的互操作性，其成员囊括了超过 500 家通信行业的运营商和组件/设备制造商。

目前已推出的比较成熟的标准有两个：一个是 2004 年颁布的 IEEE 802.16d，这个标准支持无线固定接入，也叫做固定 WiMAX；另一个是 2005 年颁布的 IEEE 802.16e，是在前一标准的基础上增加了对移动性的支持，所以也称为移动 WiMAX。

WiMAX 技术主要有两个应用领域：一个是作为蜂窝网络、Wi-Fi 热点和 Wi-Fi Mesh 的回程链路；另一个是作为最后一公里的无线宽带接入链路。

在无线宽带接入方面，WiMAX 比 Wi-Fi 的覆盖范围更大，数据速率更高。同时，WiMax 较之 Wi-Fi 具有更好的可扩展性和安全性，从而能够实现电信级的多媒体通信服务。高带宽可以补偿 IP 网络的缺陷，从而使VoIP的服务质量大大提高。

移动 WiMAX（IEEE 802.16e）向下兼容 IEEE 802.16d，在移动性方面定位的目标速率为车速，可以支持 120km/h 的移动速率。当移动速度较高时，由于多谱勒频移造成系统性能下降，因此必须在移动速率、带宽和覆盖范围之间进行权衡折衷。3G 技术强调地域上的全覆盖和高速的移动性，强调“无所不在”的服务，而 IEEE 802.16 则牺牲了全覆盖，仅保证在一定区域内实现连续覆盖，从而换取了数据传输速率的提高。

**参考答案**

（67）D

**试题（68）**

安全电子邮件使用__（68）__协议。

（68）A. PGP　　B. HTTPS　　C. MIME　　D. DES

**试题（68）分析**

PGP（Pretty Good Privacy）是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。现在 PGP 已经成为使用最广泛的电子邮件加密软件。PGP 提供两种服务：数据加密和数字签名。数据加密机制可以应用于本地存储的文件，也可以应用于网络上传输的电子邮件。数字签名机制用于数据源身份认证和报文完整性验证。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA（128 位密钥）进行数据加密，使用 MD5 进行数据完整性验证。

PGP 进行身份认证的过程叫作公钥指纹（Public-Key Fingerprint）。所谓指纹，就是对密钥进行 MD5 变换后所得到的字符串。假如 Alice 能够识别 Bob 的声音，则 Alice 可以设法得到 Bob 的公钥，并生成公钥指纹，通过电话验证他得到的公钥指纹是否与 Bob 的公钥指纹一致，以证明 Bob 公钥的真实性。

**参考答案**

（68）A

**试题（69）**

建筑物综合布线系统中的园区子系统是指__（69）__。

（69）A. 由终端到信息插座之间的连线系统
　　B. 楼层接线间到工作区的线缆系统
　　C. 各楼层设备之间的互连系统
　　D. 连接各个建筑物的通信系统

**试题（69）分析**

结构化综合布线系统（Structure Cabling System）是基于现代计算机技术的通信物理平台，集成了语音、数据、图像和视频的传输功能，消除了原有通信线路在传输介质上的差别。

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统。

（1）工作区子系统（Work Location）。

工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器以及传感器等多种终端设备。

（2）水平布线子系统（Horizontal）。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平子系统的作用是将干线子系统线路延伸到用户工作区。

（3）管理子系统（Administration）。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆互连，这些短线被称为跳线。通过跳线的调整，可以在工作区的信息插座和交换机端口之间进行连接切换。

（4）干线子系统（Backbone）。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。

（5）设备间子系统（Equipment）。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX、网络设备和监控设备等）之间的连接。

（6）建筑群子系统（Campus）。

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。大楼之间的布线方法有三种：一种是地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各种规定，安装时至少应预留 1～2 个备用管孔，以备扩充之用。第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志。最后一种是架空明线，这种方法需要经常维护。

**参考答案**

（69）D

**试题（70）**

下面有关 RMON 的论述中，错误的是__（70）__。

（70）A. RMON 的管理信息库提供整个子网的管理信息

B. RMON 的管理信息库属于 MIB-2 的一部分

C. RMON 监视器可以对每个分组进行统计和分析

D. RMON 监视器不包含 MIB-2 的功能

**试题（70）分析**

通常用于监视整个网络通信情况的设备叫作网络监视器（Monitor）或网络分析器（Analyzer）、探测器（Probe）等。监视器观察 LAN 上出现的每个分组，并进行统计和总结，给管理人员提供重要的管理信息。监视器还能存储部分分组，供以后分析用。监视器也根据分组类型进行过滤并捕获特殊的分组。通常是每个子网配置一个监视器，并且与中央管理站通信，因此叫作远程监视器。

RMON 定义了远程网络监视的管理信息库（属于 MIB-2 的一部分），以及 SNMP 管

理站与远程监视器之间的接口。一般地说，RMON 的目标就是监视子网范围内的通信，从而减少管理站和被管理系统之间的通信负担。

**参考答案**

（70）D

**试题（71）～（75）**

The TCP protocol is a __（71）__ layer protocol. Each connection connects two TCPs that may be just one physical network apart or located on opposite sides of the globe. In other words, each connection creates a __（72）__ with a length that may be totally different from another path created by another connection. This means that TCP cannot use the same retransmission time for all connections. Selecting a fixed retransmission time for all connections can result in serious consequences. If the retransmission time does not allow enough time for a __（73）__ to reach the destination and an acknowledgment to reach the source, it can result in retransmission of segment that are still on the way. Conversely, if the retransmission time is longer than necessary for a short path, it may result in delay for the application programs.

Even for one single connection, the retransmission time should not be fixed. A connection may be able to send segments and receive __（74）__ faster during nontraffic period than during congested periods. TCP uses the dynamic retransmission time, a transmission time is different for each connection and which may be changed during the same connection. Retransmission time can be made __（75）__ by basing it on the round-trip time (RTT). Several formulas are used for this purpose.

（71）A. physical　B. network　C. transport　D. application

（72）A. path　B. window　C. response　D. process

（73）A. process　B. segment　C. program　D. user

（74）A. connections　B. requests

C. acknowledgments　D. datagrams

（75）A. error　B. short　C. fixed　D. dynamic

**参考译文**

TCP 是一种传输层协议。每一个连接都连接了两个 TCP 实体，这两个 TCP 实体可能存在于同一个物理网络中，也可能是分居于地球的两边。换言之，每一个连接都产生了一条通路，其长度与另外一个连接产生的通路完全不同。这就意味着，TCP 不能对所有的连接使用同样的重传时间。对所有的连接选择一个固定的重传时间可能产生严重的后果。如果重传时间不足以使一个段到达目标，或者不足以使一个应答到达源站，这就可能对尚在路途中的段产生重传。反之，如果重传时间比一条短通路所需要的时间长，则可能对应用程序产生延迟。

即使对单个连接，重传时间也不应该固定。一个连接应该能够在非峰值时段比拥堵时段更快地发送数据段和接收应答。TCP 使用了动态重传时间，重传时间对每一个连接是不同的，在同一个连接持续期间也是可以改变的。重传时间可以动态地根据环回时间（RTT）而改变。为此建立了几个有用的公式。

**参考答案**

（71）C　（72）A　（73）B　（74）C　（75）D

# 第 14 章　2012 上半年网络工程师下午试题分析与解答

**试题一（共 15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司计划部署园区网络，其建筑物分布如图 1-1 所示。

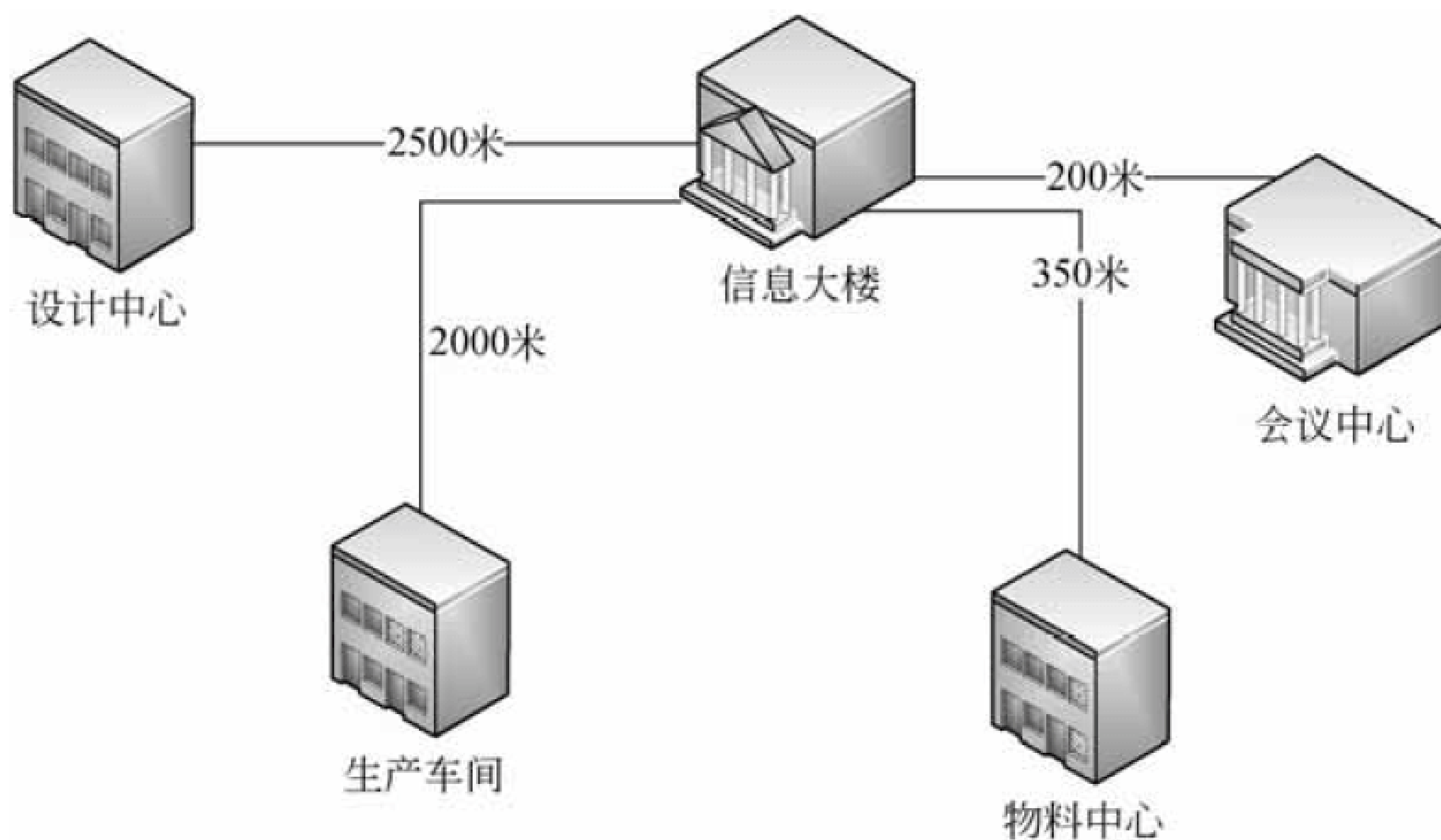



图 1-1

根据需求分析结果，网络规划要求如下：

1．网络中心机房在信息大楼。

2．设计中心由于业务需求，要求千兆到桌面；同时要求设计中心汇聚交换机到核心交换机以千兆链路聚合。

3．会议中心采用 PoE 无线网络部署。

**【问题 1】（5 分，每空 1 分）**

根据公司网络需求分析，设计人员设计的网络拓扑结构如图 1-2 所示。

1．根据网络需求描述和网络拓扑结构，图 1-2 中介质 1 应选用__（1）__；介质 2 应选用__（2）__；介质 3 应选用__（3）__。

（1）～（3）备选答案：（注：每项只能选择一次）

A. 单模光纤

B. 多模光纤

C. 6 类双绞线

D. 同轴电缆

2．在该网络中，应至少选用单模 SFP__（4）__个，多模 SFP__（5）__个。

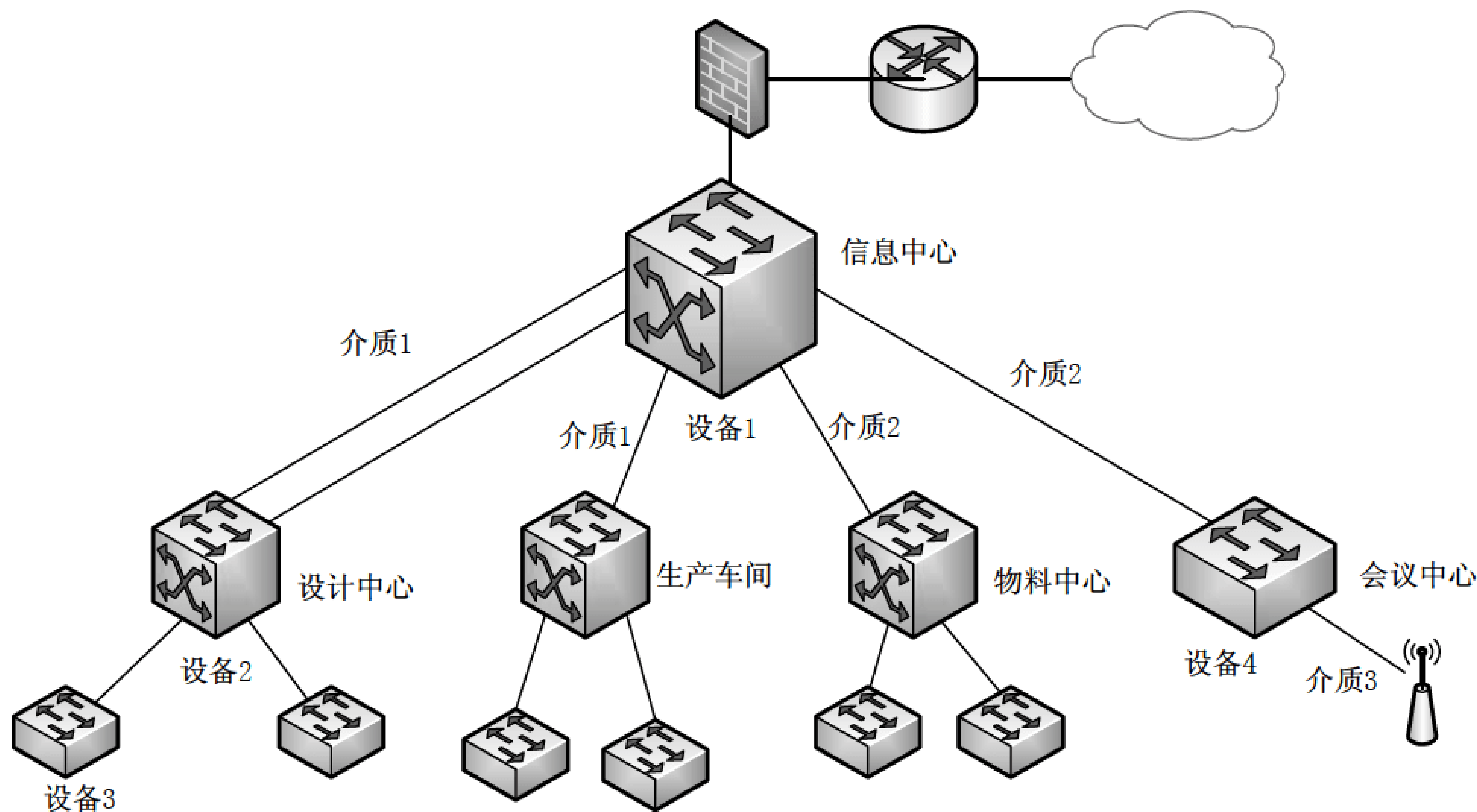



图 1-2

**【问题 2】（4 分，每空 1 分）**

该网络部分设备如下表所示：

| 名称 | 主要技术指标 |
|---|---|
| 设备 A | 交换容量≥1Tbps；包转发率≥750Mpps；业务插槽数≥6；双引擎，冗余电源；配置接口≥12 口千兆光口，≥24 口千兆电口 |
| 设备 B | 交换容量≥190Gbps；包转发率≥40Mpps；接口为 24 个 10/100/1000M 电口；至少有 2 个 1000M SFP 光口；支持 802.1x 认证，MAC 认证和 Web 认证 |
| 设备 C | 交换容量≥70Gbps；包转发率≥40Mpps；接口为 24 个 10/100/1000M 电口，2 个 1G SFP；可管理 AP 数目≥16；支持高级加密标准（AES）、临时密钥交换协议（TKIP）以及有线对等加密（WEP）、支持 WPA 及 WPA2 加密算法；防止 ARP 欺骗攻击 |
| 设备 D | 交换容量≥268Gbps；包转发率≥150Mpps；接口为 24 个 10/100/1000Base-T 以太网端口，4 个 1/10G SFP |

根据题目说明和网络拓扑图，在图 1-2 中，设备 1 应选用<u>（6）</u>，设备 2 应选用<u>（7）</u>，设备 3 应选用<u>（8）</u>，设备 4 应选用<u>（9）</u>。

**【问题 3】（6 分，每空 1 分）**

该网络在进行地址分配时，其 VLAN 分配如下表所示：

| 设备 | 端口连接设备 | | IP | 网关 | VLAN ID |
|---|---|---|---|---|---|
| | 设备名称 | 接口号 | | | |
| 生产车间汇聚交换机 | 核心交换机 | g2/1 | | | TRUNK |
| | 接入交换机 A | f1/2 | 192.168.99.0/24 | 192.168.99.254 | VLAN 99 |
| | 接入交换机 B | f1/3 | 192.168.100.0/24 | 192.168.100.254 | VLAN 100 |
| | 管理地址 | | 192.168.1.11/24 | 192.168.1.254 | VLAN 1 |

根据上表，完成下列生产车间汇聚交换机的配置：

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface vlan 100
Switch(config-if)#ip address  (10)    (11) 
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface f1/2
Switch(config-if)#switchport mode  (12) 
Switch(config-if)#switchport access vlan  (13) 
Switch(config-if)#exit

Switch(config)#interface g2/1
Switch(config-if)#switchport mode  (14) 
Switch(config-if)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway  (15) 
…
```

## 试题一分析

本题考查网络规划的基本知识与应用。

**【问题 1】**

根据题目说明和建筑物分布图可知，网络中心机房在信息大楼；信息大楼距离设计中心 2500 米；信息大楼距离生产车间 2000 米；信息大楼距离物料中心 350 米；信息大楼距离会议中心 200 米。

由于距离的问题，介质 1（信息大楼至设计中心和生产车间）只能选择单模光纤，介质 2（信息大楼至会议中心和物料中心）可以选择单模光纤和多模光纤，但是题目要求选项只能单选，所以此处只能选择多模光纤；介质 3（会议中心交换机至 AP）由于会议中心采用 PoE 无线网络部署，因此此处只能选择 6 类双绞线。

另外，设计中心汇聚交换机到核心交换机以千兆链路聚合，所以信息大楼至设计中心为双路光纤，这样可以判断在该网络中，应至少选用单模 SFP 6 个，多模 SFP4 个。

【问题 2】

根据设备表可知，设备 A 属于核心交换设备；设备 B 属于接入交换设备；设备 C 属于无线管理设备；设备 D 属于汇聚交换设备。再根据网络拓扑图，在图 1-2 中，设备 1 应选用核心交换设备（设备 A），设备 2 应选用汇聚交换设备（设备 D），设备 3 应选用接入交换设备（设备 B），设备 4 应选用无线管理设备（设备 C）。

【问题 3】

本问题考查的是 VLAN 分配应用的基础知识。根据 VLAN 分配表，生产车间汇聚交换机的配置应如下：

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface vlan 100
Switch(config-if)#ip address 192.168.100.254  255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface f1/2
Switch(config-if)#switchport mode  access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit

Switch(config)#interface g2/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.254
…
```

## 参考答案

【问题 1】

（1）A. 单模光纤

（2）B. 多模光纤

（3）C. 6 类双绞线

（4）6

（5）4

**【问题 2】**

（6）设备 A

（7）设备 D

（8）设备 B

（9）设备 C

**【问题 3】**

（10）192.168.100.254

（11）255.255.255.0

（12）access

（13）99

（14）trunk

（15）192.168.1.254

**试题二（15 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【问题 1】（3 分，每空 1.5 分）**

Linux 服务器中 DHCP 服务程序/usr/sbin/dhcpd 对应的配置文件名称是__（1）__，该文件的缺省目录是__（2）__。

**【问题 2】（6 分，每空 1 分）**

某网络采用 Linux DHCP 服务器为主机提供服务，查看某主机的网络连接详细信息如图 2-1 所示。

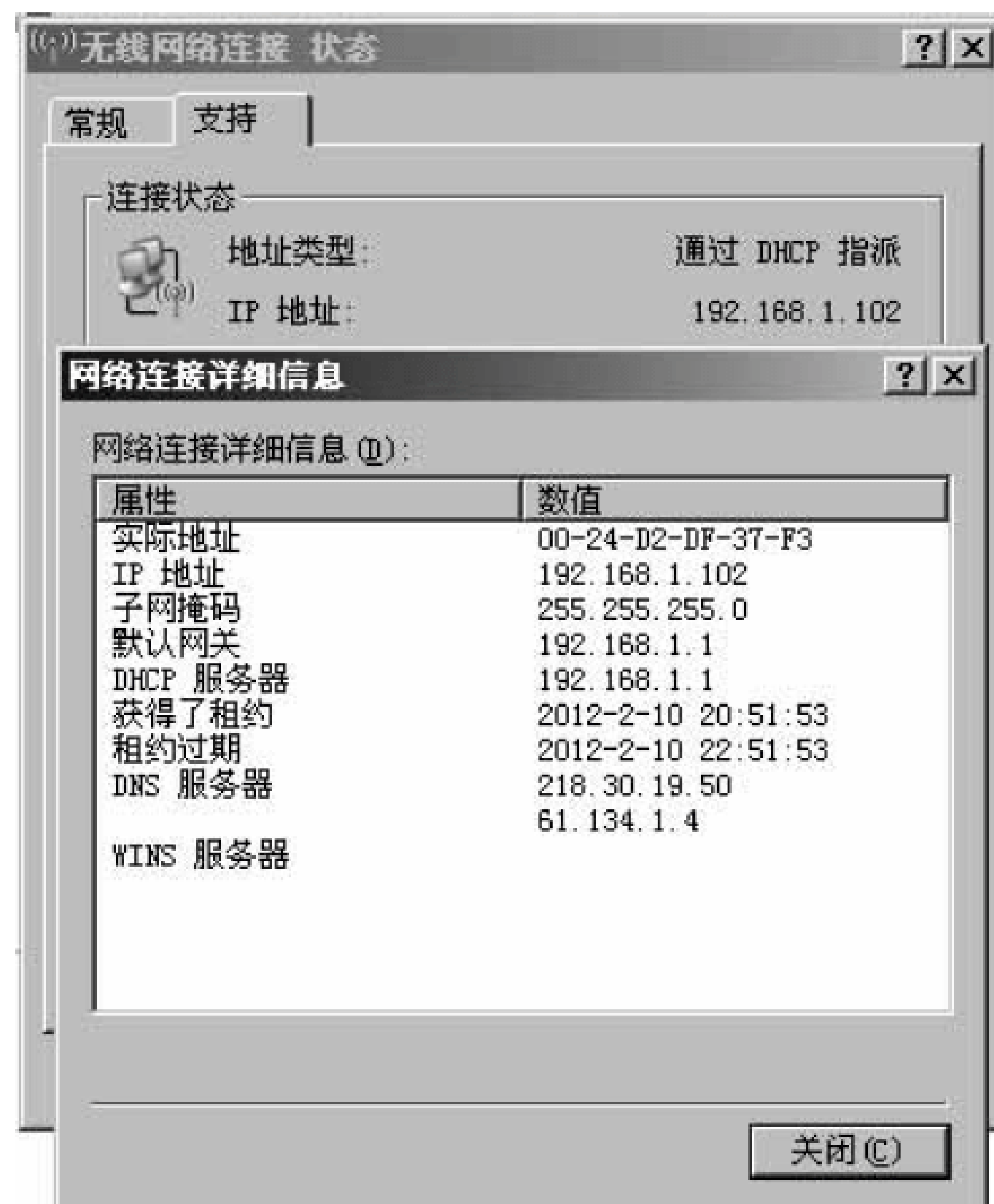



图 2-1

请根据图 2-1 中补充完成 Linux DHCP 服务器中 DHCP 配置文件的相关配置项。

```
…
subnet 192.168.1.0  netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.200;
default-lease-time （3）;
max-lease-time  14400;
option subnet-mask （4）;
option routers （5）;
option domain-name "myuniversity.edu.cn";
option broadcast-address （6）;
option domain-name-servers （7） , （8）;
}
```

**【问题 3】（6 分，每空 2 分）**

如果要确保 IP 地址 192.168.1.102 分配给图 2-1 中的 PC，需要在 DHCP 配置文件中补充以下语句。

（9） pc1{hardware ethernet （10） ; fixed-address （11） ;}

**试题二分析**

本题考查 Linux 系统中 DHCP 服务的相关配置。

DHCP 是 Dynamic Host Configuration Protocol（动态主机配置协议）的缩写。在常见的小型网络中，IP 地址的分配一般都采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址的方式会加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP 服务是非常有效率的。

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，DHCP 配置通常包括三部分：parameters、declarations、option。

parameters 用于说明 DHCP 服务工作的网络配置参数，如下表所示。

| 参　　数 | 参 数 含 义 |
|---|---|
| ddns-update-style | 配置 DHCP-DNS 更新模式。更新模式包括 none、interim 和 ad-hoc |
| default-lease-time | 指定缺省的 IP 地址租赁时间，单位是秒 |
| max-lease-time | 指定最大租赁时间长度，单位是秒 |
| hardware | 指定网卡接口类型和 MAC 地址 |
| server-name | DHCP 服务器名称 |
| get-lease-hostnames flag | 检查客户端使用的 IP 地址 |
| fixed-address ip | 分配给客户端一个固定的地址 |
| authritative | 拒绝不正确的 IP 地址请求 |

declarations 用来描述网络布局、提供 DHCP 客户的 IP 地址分配策略等，如下表所示。

| 声　明 | 参 数 含 义 |
| --- | --- |
| shared-network | 用来设置是否一些 IP 子网共享同一物理网络 |
| subnet | 描述一个 IP 地址是否属于该子网 |
| range | 提供动态分配 IP 的范围 |
| host | 用于定义保留主机 |
| group | 为一组参数提供声明 |
| Allow unknown-clients;<br>deny unknown-client | 是否动态分配 IP 给未知的使用者 |
| allow bootp;deny bootp | 是否响应 BOOTP 查询 |
| Allow booting;deny booting | 是否响应 TFTP 查询，主要用于无盘工作站 |
| filename | 启动文件的名称，主要用于无盘工作站 |
| next-server | 设置 TFTP 服务器的地址，主要用于无盘工作站 |

option（选项）用来配置 DHCP 可选参数，用 option 关键字作为开始，如下表所示。

| 选　项 | 解　释 |
| --- | --- |
| subnet-mask | 为客户端设定子网掩码 |
| domain-name | 为客户端指明 DNS 名字 |
| domain-name-servers | 为客户端指明 DNS 服务器 IP 地址 |
| host-name | 为客户端指定主机名称 |
| routers | 为客户端设定默认网关 |
| broadcast-address | 为客户端设定广播地址 |
| ntp-server | 为客户端设定网络时间服务器 IP 地址 |
| time－offset | 为客户端设定和格林威治时间的偏移时间，单位是秒 |

【问题 1】

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，所以 DHCP 服务对应的配置文件名称是 dhcpd.conf，缺省目录是/etc。

【问题 2】

由图 2-1 可知，default-lease-time 为租约过期时间减去获取租约时间，等于 2 小时，合计 7200 秒。

【问题 3】

host 语句用于保留主机的设置，参数是保留主机的 MAC 地址和对应分配的 IP 地址。

**参考答案**

【问题 1】

（1）dhcpd.conf

（2）/etc

【问题 2】

（3）7200

（4）255.255.255.0

（5）192.168.1.1

（6）192.168.1.255

（7）218.30.19.50

（8）61.134.1.4

【问题 3】

（9）host

（10）00:24:D2:DF:37:F3

（11）192.168.1.102

**试题三（共 15 分）**

阅读下列说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】

网络拓扑结构如图 3-1 所示，其中 Web 服务器 WebServer1 和 WebServer2 对应同一域名 www.abc.com，DNS 服务器采用 Windows Server 2003 操作系统。

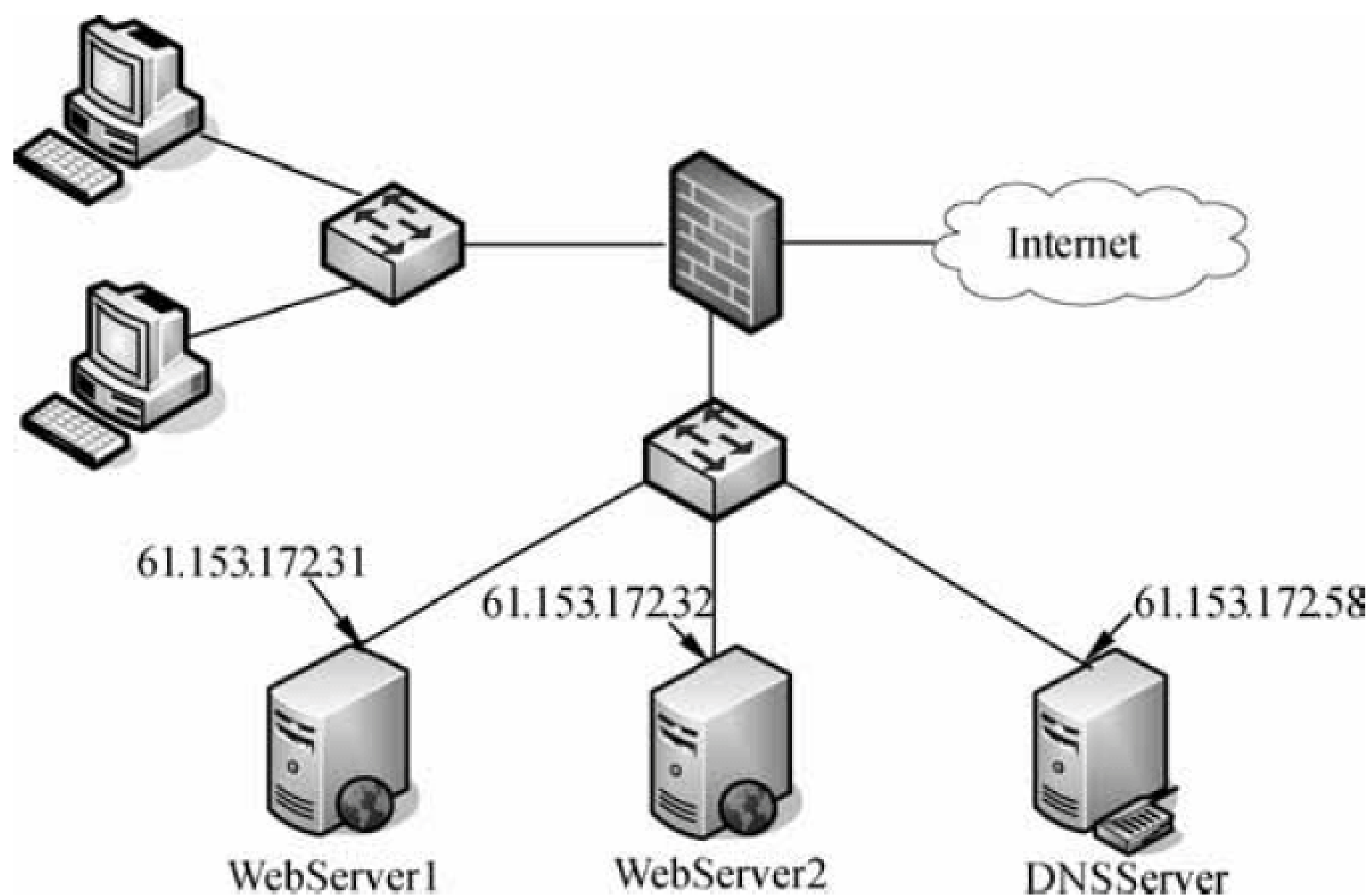



图 3-1

【问题 1】（2 分）

客户端向 DNS 服务器发出解析请求后，没有得到解析结果，则＿（1）＿进行解析。

（1）备选答案：

A．查找本地缓存　　B．使用 NetBIOS 名字解析

C．查找根域名服务器　　D．查找转发域名服务器

**【问题 2】（2 分）**

在图 3-1 中，两台 Web 服务器采用同一域名的主要目的是什么？

**【问题 3】（3 分，每空 1.5 分）**

DNS 服务器为 WebServer1 配置域名记录时，在图 3-2 所示的对话框中，添加的主机“名称”为__（2）__，“IP 地址”是__（3）__。

采用同样的方法为 WebServer2 配置域名记录。

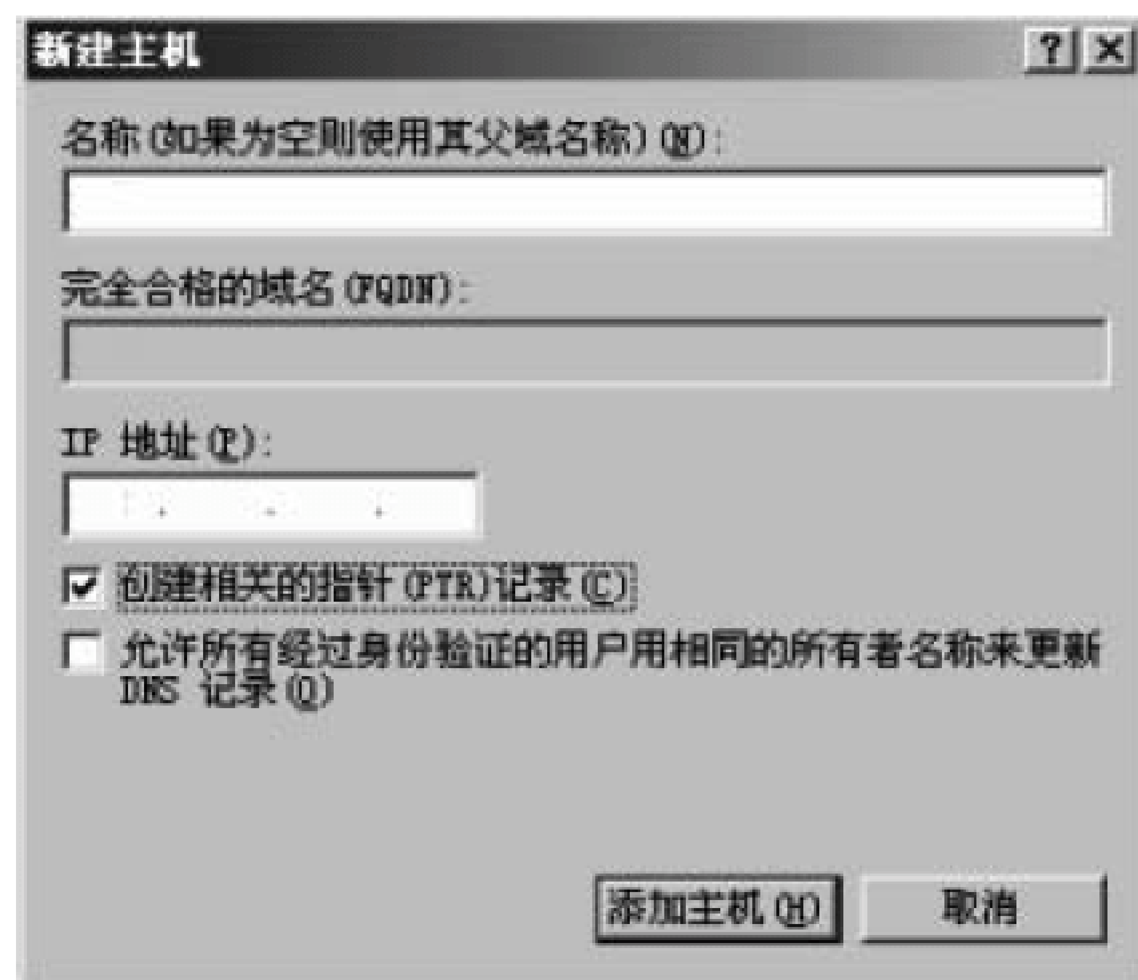



图 3-2

**【问题 4】（4 分）**

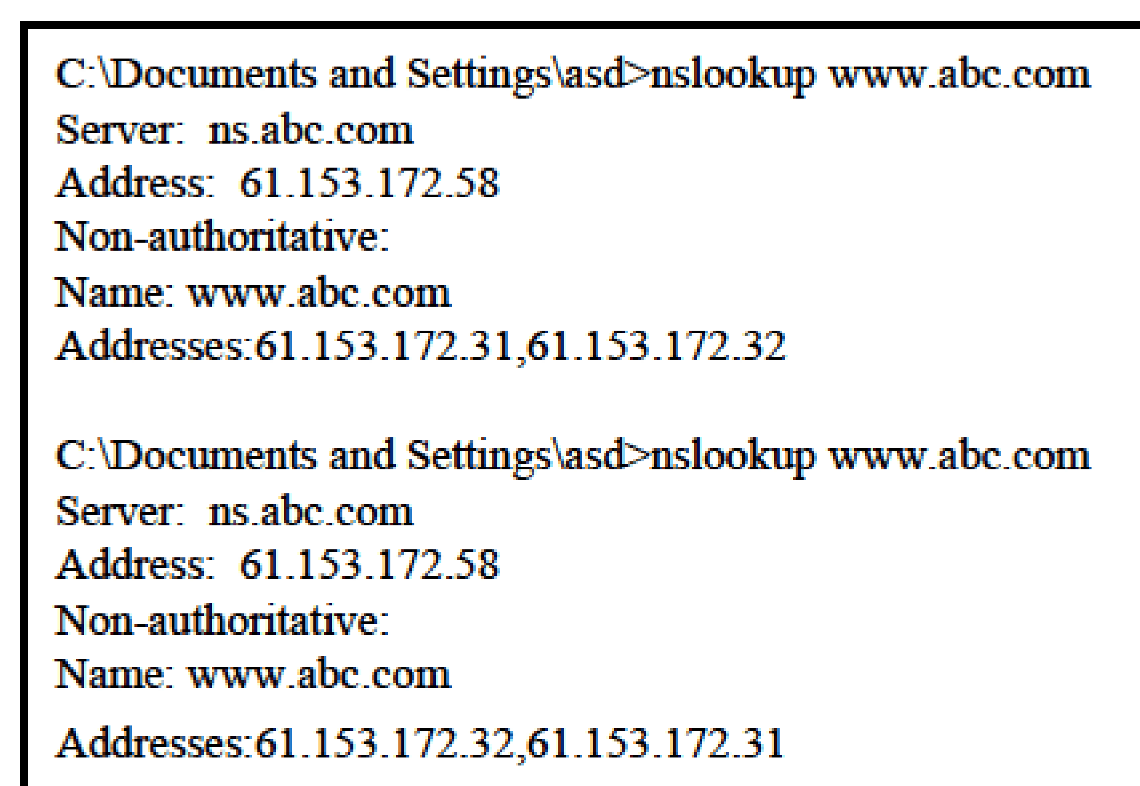
在 DNS 系统中，反向查询（Reverse Query）的功能是__（4）__。若不希望对域名 www.abc.com 进行反向查询，在图 3-2 所示的窗体中应如何操作？

**【问题 5】（2 分）**

在图 3-3 中所示的 DNS 服务器属性窗口中应如何配置，才使得两次使用 nslookup www.abc.com 命令得到如图 3-4 所示结果？




图 3-3



```
C:\Documents and Settings\asd>nslookup www.abc.com
Server:  ns.abc.com
Address:  61.153.172.58
Non-authoritative:
Name: www.abc.com
Addresses:61.153.172.31,61.153.172.32

C:\Documents and Settings\asd>nslookup www.abc.com
Server:  ns.abc.com
Address:  61.153.172.58
Non-authoritative:
Name: www.abc.com
Addresses:61.153.172.32,61.153.172.31
```

图 3-4

**【问题 6】（2 分，每空 1 分）**

要测试 DNS 服务器是否正常工作，在客户端可以采用的命令是__（5）__或__（6）__。

（5）、（6）备选答案：

A．ipconfig　　B．nslookup　　C．ping　　D．netstat

**试题三分析**

本题考查 Windows Server 2003 系统中 DNS 服务器的配置。

**【问题 1】**

DNS 主机名解析的查找顺序是：先查找客户端解析程序缓存；如果没有成功，则向 DNS 服务器发出解析请求；如果还没有成功，则尝试使用 NetBIOS 名字解析方法取得结果。

**【问题 2】**

两台 Web 服务器采用同一域名有两个好处：首先，对同一域名进行解析时可以由 DNS 服务器采用某种策略均衡到两台 Web 服务器上，对 Web 服务实现负载均衡；其次，当某一台服务器产生故障时可以由另一台提供服务，可防止单点失效。

**【问题 3】**

DNS 服务器为 WebServer1 配置域名记录时，添加的主机“名称”栏对应的是主机名，即 WWW，“IP 地址”栏应填入提供 Web 服务的 IP 地址，即 61.153. 172.31。

**【问题 4】**

在 DNS 系统中，反向查询的功能是用 IP 地址查询对应的域名。若新建一条 DNS 记录时希望同时创建它的反向查询记录，需勾选“创建相关的指针（PTR）记录”。若不希望对域名 www.abc.com 进行反向查询，需“创建相关的指针（PTR）记录”。

**【问题 5】**

从结果图中可以看出，在解析 www.abc.com 时，循环对应到了 61.153.172.31 和 61.153. 172.32 两个主机，故在 DNS 服务器中应该配置循环功能。

**【问题 6】**

测试 DNS 服务器是否正常工作，可以采用两种方式：第一种通过 ping 域名来测试；第二种采用 nslookup 来查看提供服务的 DNS 服务器。

**参考答案**

**【问题 1】**

（1）B．使用 NetBIOS 名字解析

**【问题 2】**

对 Web 服务实现负载均衡或防止单点失效

**【问题 3】**

（2）www

（3）61.153. 172.31

**【问题 4】**

（4）用 IP 地址查询对应的域名

去掉“创建相关的指针（PTR）记录”

**【问题5】**

勾选“启用循环”

**【问题6】**

（5）B．Nslookup

（6）C．ping

注意：（5）、（6）答案可以互换

**试题四（共15分）**

阅读以下说明，回答问题1至问题4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业在部门A和部门B分别搭建了局域网，两局域网通过两台Windows Server 2003服务器连通，如图4-1所示，要求采用IPSec安全机制，使得部门A的主机PC1可以安全访问部门B的服务器S1。

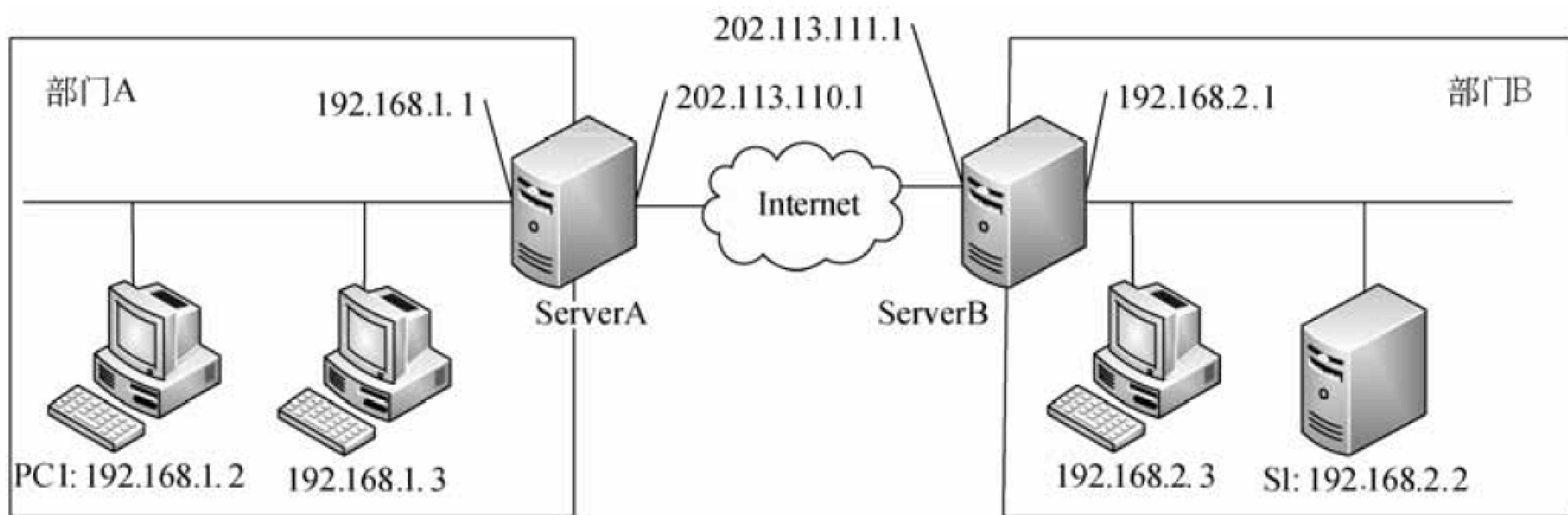



图4-1

**【问题1】（3分，每空1分）**

IPSec工作在TCP/IP协议栈的__（1）__层，为TCP/IP通信提供访问控制、数据完整性、数据源验证、抗重放攻击、机密性等多种安全服务。IPSec包括AH、ESP和ISAKMP/Oakley等协议，其中，__（2）__为IP包提供信息源和报文完整性验证，但不支持加密服务；__（3）__提供加密服务。

**【问题2】（2分）**

IPSec支持传输和隧道两种工作模式，如果要实现PC1和S1之间端到端的安全通信，则应该采用__（4）__模式。

**【问题3】（6分，每空2分）**

如果IPSec采用传输模式，则需要在PC1和__（5）__上配置IPSec安全策略。在PC1的IPSec筛选器属性窗口页中（见图4-2），源IP地址应设为__（6）__，目标IP地址应设为__（7）__。




图 4-2

**【问题 4】（4 分，每空 1 分）**

如果要保护部门 A 和部门 B 之间所有的通信安全，则应该采用隧道模式，此时需要在 ServerA 和＿（8）＿上配置 IPSec 安全策略。

在 ServerA 的 IPSec 筛选器属性窗口页中（见图 4-3），源 IP 子网的 IP 地址应设为＿（9）＿，目标子网 IP 地址应设为＿（10）＿，源地址和目标地址的子网掩码均设为 255.255.255.0。ServerA 的 IPSec 规则设置中（见图 4-4），指定的隧道端点 IP 地址应设为＿（11）＿。

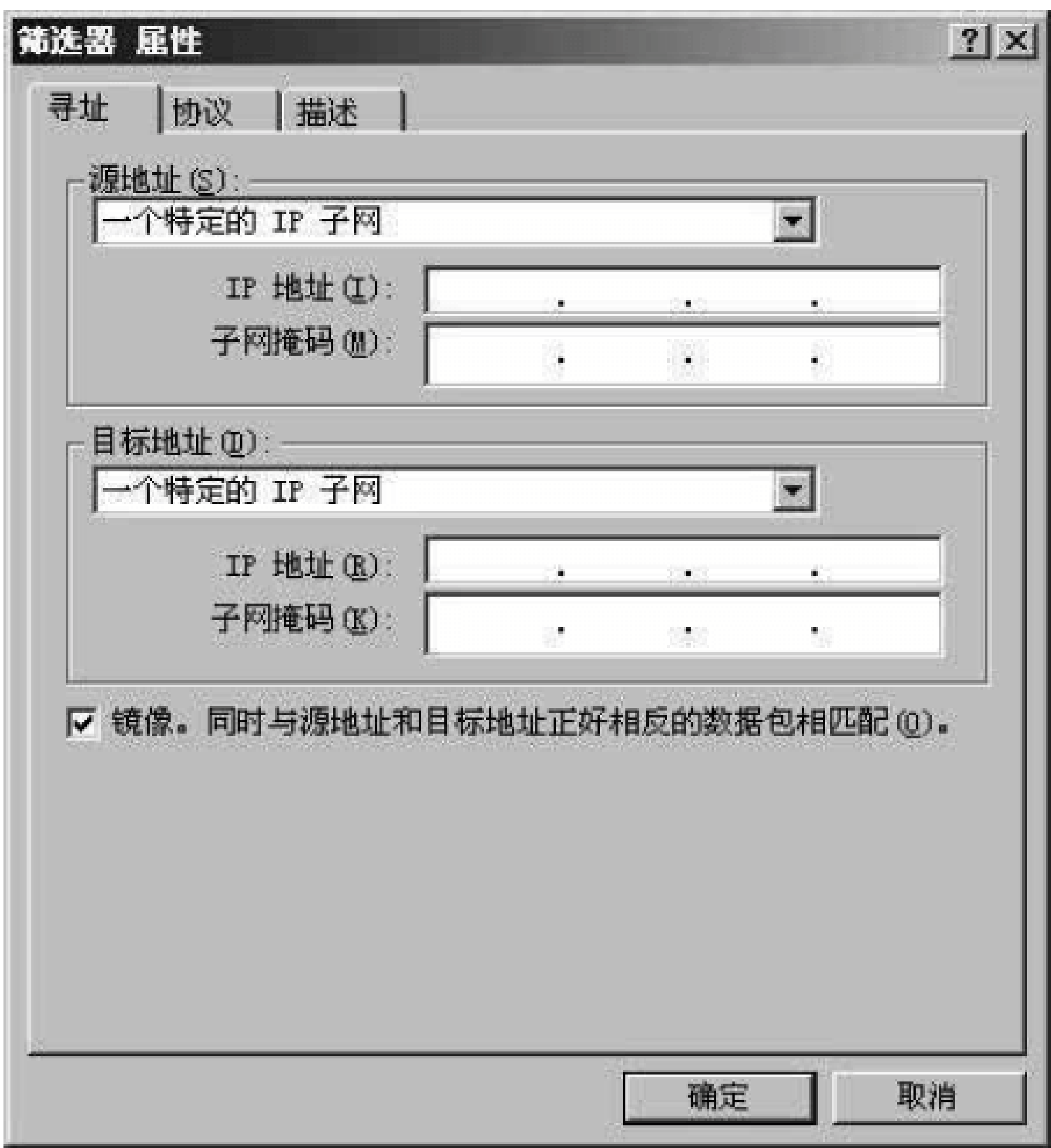



图 4-3

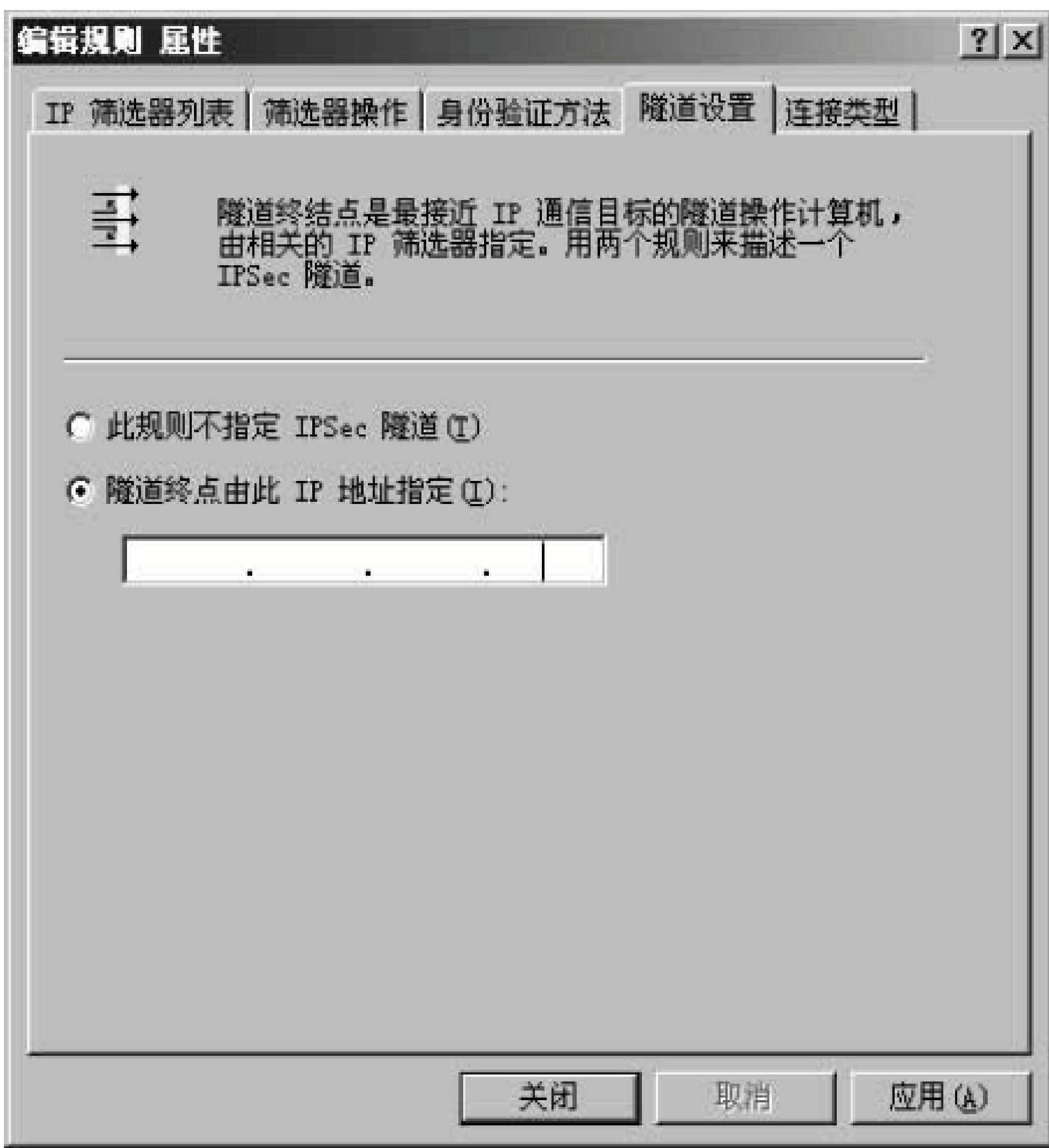



图 4-4

**试题四分析**

本题考查 IPSec 的工作原理和 Windows Server 2003 中 IPSec 的配置。

**【问题 1】**

IPsec（IP Security）是 IETF 定义的一组协议，用于增强 IP 网络的安全性。其功能可以划分为下面三类：

- 认证头（Authentication Header，AH）：用于数据完整性认证和数据源认证。
- 封装安全负荷（Encapsulating Security Payload，ESP）：提供数据保密性和数据完整性认证。ESP 也包括了防止重放攻击的顺序号。
- Internet 密钥交换协议（Internet Key Exchange，IKE）：用于生成和分发在 ESP 和 AH 中使用的密钥。IKE 也对远程系统进行初始认证。

因此，IPSec 工作在 TCP/IP 协议栈的 IP 层，AH 为 IP 包提供信息源和报文完整性验证，但不支持加密服务，ESP 提供加密服务。

**【问题 2】**

IPSec 支持传输和隧道两种工作模式，其中传输模式一般用于主机到主机之间端到端的安全通信，隧道模式用于网关到网关之间的安全通信。

**【问题 3】**

如果 IPSec 采用传输模式，则需要在通信的两个端点 PC1 和 S1 上配置 IPSec 安全策略。在 PC1 的 IPSec 筛选器属性窗口页中，源 IP 地址应设为 PC1 自身的 IP 地址 192.168.1.2，目标 IP 地址应设为 S1 的 IP 地址 192.168.2.2。

**【问题 4】**

如果要保护部门 A 和部门 B 之间所有的通信安全，应该采用隧道模式，此时需要在部门 A 和部门 B 的网关 ServerA 和 ServerB 上配置 IPSec 安全策略。

在 ServerA 的 IPSec 筛选器属性窗口页中，源 IP 子网的 IP 地址应设为部门 A 所在子网 192.168.1.0，目标子网 IP 地址应设为部门 B 所在子网 192.168.2.0。ServerA 的 IPSec 规则设置中，指定的隧道端点应该为部门 B 网关的公网地址 202.113.111.1。

**参考答案**

**【问题 1】**

（1）IP（网络）

（2）AH

（3）ESP

**【问题 2】**

（4）传输

**【问题 3】**

（5）S1 或 192.168.2.2

（6）192.168.1.2

（7）192.168.2.2

**【问题 4】**

（8）ServerB 或 202.113.111.1

（9）192.168.1.0

（10）192.168.2.0

（11）202.113.111.1

**试题五（共 15 分）**

阅读以下说明，回答问题 1 至问题 2，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司总部内采用 RIP 协议，网络拓扑结构如图 5-1 所示。根据业务需求，公司总部的 192.168.40.0/24 网段与分公司 192.168.100.0/24 网段通过 VPN 实现互联。

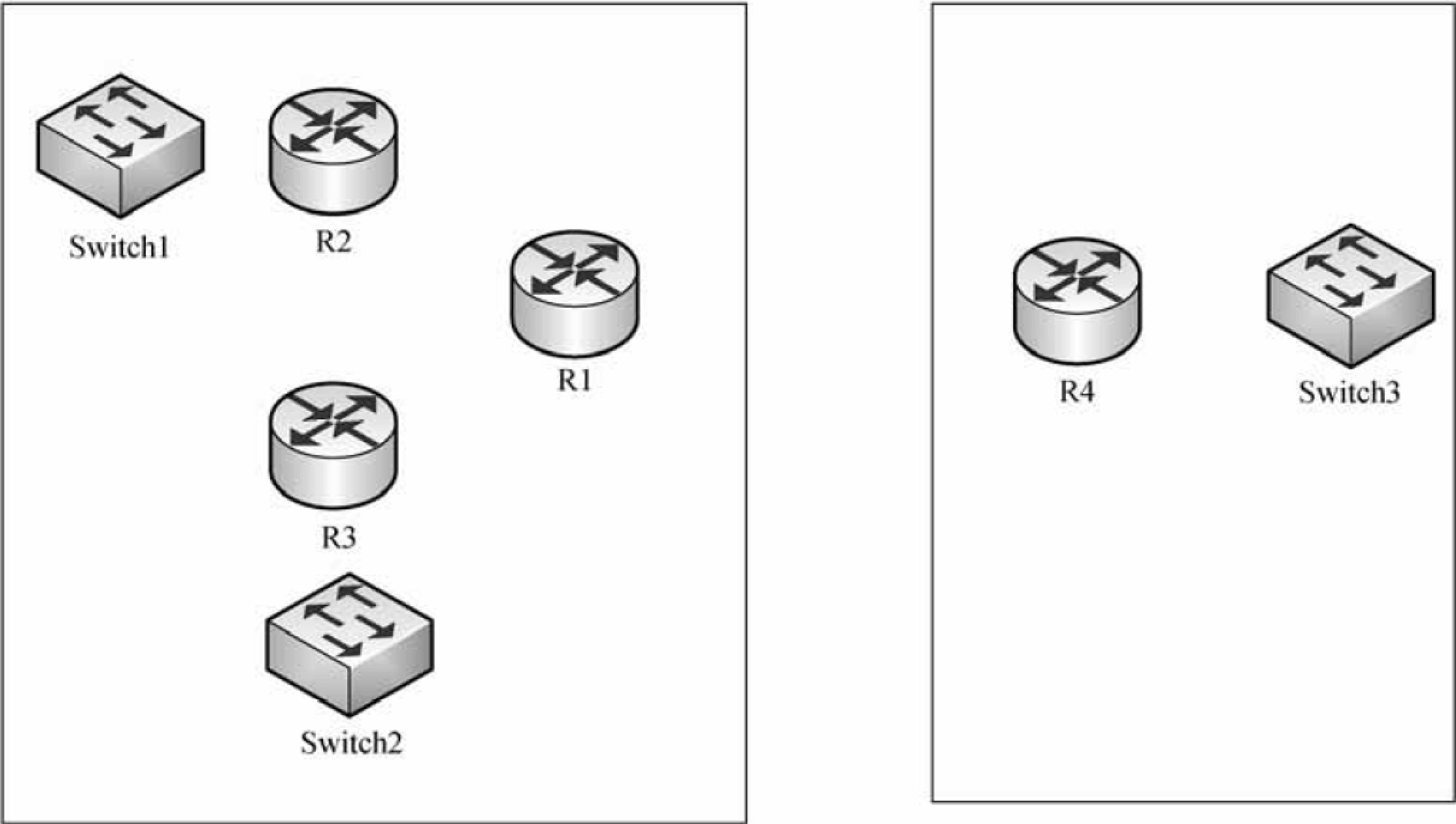



图 5-1

在网络拓扑图中的路由器各接口地址如下表所示。

| 名称 | 接口 | IP |
| --- | --- | --- |
| R1 | S0/0 | 212.34.17.9/27 |
| R1 | S0/1 | 192.168.10.1/24 |
| R1 | S0/2 | 192.168.20.1/24 |
| R2 | S0/0 | 192.168.10.2/24 |
| R2 | S0/1 | 192.168.30.1/24 |

续表

| 名称 | 接口 | IP |
|---|---|---|
| R2 | F1/1 | 192.168.40.1/24 |
| R3 | S0/0 | 192.168.20.2/24 |
| R3 | S0/1 | 192.168.30.2/24 |
| R3 | F1/1 | 192.168.50.1/24 |
| R4 | S0/0 | 202.100.2.3/27 |
| R4 | F1/1 | 192.168.100.1/24 |

**【问题 1】（6 分，每空 1 分）**

根据网络拓扑和需求说明，完成路由器 R2 的配置：

```
R2#config t
R2 (config)#interface serial 0/0
R2 (config-if)#ip address  (1)   (2)
R2 (config-if)#no shutdown
R2(config-if)#exit
R2 (config)#ip routing
R2 (config)#router  (3)                ;（进入 RIP 协议配置子模式）
R2 (config-router)#network  (4)
R2 (config-router)#network  (5)
R2 (config-router)#network  (6)
R2 (config-router)#version 2           ;（设置 RIP 协议版本 2）
R2(config-router)#exit
```

**【问题 2】（9 分，每空 1.5 分）**

根据网络拓扑和需求说明，完成（或解释）路由器 R1 的配置。

```
R1(config)# interface serial 0/0
R1(config-if)# ip address  (7)   (8)
R1(config-if)# no shutdown
R1(config)#ip route 192.168.100.0 0.0.0.255 202.100.2.3; (9)
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share              ; (10)
R1(config-isakmp)#encryption 3des        ;加密使用 3DES 算法
R1(config-isakmp)#hash md5               ;定义 MD5 算法
R1(config)#crypto isakmp key test123 address  (11)
                                         ;设置密钥为 test123 和对端地址
R1(config)#crypto isakmp transform-set link ah-md5-h esp-3des
                                         ;指定 VPN 的加密和认证算法
```

```
R1(config)#access-list 300 permit ip 192.168.100.0 0.0.0.255
                                        ;配置 ACL
R1(config)#crypto map vpntest 1 ipsec-isakmp
                                        ;创建 crypto map 名字为 vpntest
R1(config-crypto-map)#set peer 202.100.2.3          ;指定链路对端 IP 地址
R1(config-crypto-map)#set transfrom-set link        ;指定传输模式 link
R1(config-crypto-map)#match address 300             ;指定应用访控列表
R1(config)# interface serial 0/0
R1(config)#crypto map （12）                         ;应用到接口
```

**试题五分析**

本题考查路由器配置的基本知识。

**【问题 1】**

根据题目说明和路由器各接口地址表可知，在公司总部路由器 R2 的 RIP 配置应如下：

```
R2#config t
R2 (config)#interface serial 0/0
R2 (config-if)#ip address  192.168.10.2  255.255.255.0
R2 (config-if)#no shutdown
R2(config-if)#exit
R2 (config)#ip routing
R2 (config)#router RIP                      ；（进入 RIP 协议配置子模式）
R2 (config-router)#network 192.168.10.0     ；（声明网络 192.168.10.0/24）
R2 (config-router)#network 192.168.40.0     ；（声明网络 192.168.10.0/24）
R2 (config-router)#network 192.168.30.0     ；（声明网络 192.168.10.0/24）
R2 (config-router)#version 2                ；（设置 RIP 协议版本 2）
R2(config-router)#exit
```

**【问题 2】**

本问题考查的是 vpn 配置的基础知识。根据题目说明，公司总部的 192.168.40.0/24 网段与分公司 192.168.100.0/24 网段通过 VPN 实现互联，所以路由器 VPN 配置如下：

```
R1(config)# interface serial 0/0
R1(config-if)# ip address 212.34.17.9 255.255.255.224
R1(config-if)# no shutdown
R1(config)#ip route 192.168.100.0 0.0.0.255 202.100.2.3
                                            ;配置静态路由（指向 VPN 的对端）
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share  ;定义预共享密钥
R1(config-isakmp)#encryption 3des           ;加密使用 3DES 算法
```

```
R1(config-isakmp)#hash md5                     ;定义 MD5 算法
R1(config)#crypto isakmp key test123 address 202.100.2.3
                                               ;设置密钥为 test123 和对端地址
R1(config)#crypto isakmp transform-set link ah-md5-h esp-3des
                                               ;指定 VPN 的加密和认证算法
R1(config)#accress-list 300 permit ip 192.168.100.0 0.0.0.255
                                               ;配置 ACL
R1(config)#crypto map vpntest 1 ipsec-isakmp
                                               ;创建 cryptomap 名字为 vpntest
R1(config-crypto-map)#set peer 202.100.2.3  ;指定链路对端 IP 地址
R1(config-crypto-map)#set transfrom-set link ;指定传输模式 link
R1(config-crypto-map)#match address 300      ;指定应用访控列表
R1(config)# interface serial 0/0
R1(config)#crypto map vpntest                  ;应用到接口
```

**参考答案**

**【问题 1】**

（1）192.168.10.2

（2）255.255.255.0

（3）RIP

（4）192.168.10.0

（5）192.168.40.0

（6）192.168.30.0

注意：（4）、（5）、（6）可以互换。

**【问题 2】**

（7）212.34.17.9

（8）255.255.255.224

（9）配置静态路由（指向 VPN 的对端）

（10）定义预共享密钥

（11）202.100.2.3

（12）vpntest

# 第 15 章　2012 下半年网络工程师上午试题分析与解答

**试题（1）**

在 CPU 中，__（1）__不仅要保证指令的正确执行，还要能够处理异常事件。

（1）A．运算器　　B．控制器　　C．寄存器组　　D．内部总线

**试题（1）分析**

本题考查计算机系统硬件方面的基础知识。

计算机中的 CPU 是硬件系统的核心，用于数据的加工处理，能完成各种算术、逻辑运算及控制功能。其中，控制器的作用是控制整个计算机的各个部件有条不紊地工作，它的基本功能就是从内存取指令和执行指令。

**参考答案**

（1）B

**试题（2）**

计算机中主存储器主要由存储体、控制线路、地址寄存器、数据寄存器和__（2）__组成。

（2）A．地址译码电路　　B．地址和数据总线

C．微操作形成部件　　D．指令译码器

**试题（2）分析**

本题考查存储系统基础知识。

主存储器简称为主存、内存，设在主机内或主机板上，用来存放机器当前运行所需要的程序和数据，以便向 CPU 提供信息。相对于外存，其特点是容量小速度快。

主存储器主要由存储体、控制线路、地址寄存器、数据寄存器和地址译码电路等部分组成。

**参考答案**

（2）A

**试题（3）**

以下关于数的定点表示和浮点表示的叙述中，不正确的是__（3）__。

（3）A．定点表示法表示的数（称为定点数）常分为定点整数和定点小数两种

B．定点表示法中，小数点需要占用一个存储位

C．浮点表示法用阶码和尾数来表示数，称为浮点数

D．在总位数相同的情况下，浮点表示法可以表示更大的数

**试题（3）分析**

本题考查数据表示基础知识。

各种数据在计算机中表示的形式称为机器数，其特点是采用二进制计数制，数的符号用 0、1 表示，小数点则隐含表示而不占位置。机器数对应的实际数值称为数的真值。

为了便于运算，带符号的机器数可采用原码、反码、补码和移码等不同的编码方法。

所谓定点数，就是表示数据时小数点的位置固定不变。小数点的位置通常有两种约定方式：定点整数（纯整数，小数点在最低有效数值位之后）和定点小数（纯小数，小数点在最高有效数值位之前）。

当机器字长为 n 时，定点数的补码和移码可表示 2^$n$ 个数，而其原码和反码只能表示 2^$n$−1 个数（0 表示占用了两个编码），因此，定点数所能表示的数值范围比较小，运算中很容易因结果超出范围而溢出。

数的浮点表示形式为：$N = 2^E \times F$，其中，$E$ 称为阶码，$F$ 为尾数。阶码通常为带符号的纯整数，尾数为带符号的纯小数。浮点数的表示格式如下：

| 阶符 | 阶码 | 数符 | 尾数 |
|---|---|---|---|

很明显，一个数的浮点表示不是唯一的。当小数点的位置改变时，阶码也相应改变，因此可以用多种浮点形式表示同一个数。

浮点数所能表示的数值范围主要由阶码决定，所表示数值的精度则由尾数决定

**参考答案**

（3）B

**试题（4）**

X、Y 为逻辑变量，与逻辑表达式 $X+\overline{X}Y$ 等价的是＿（4）＿。

（4）A. $X+\overline{Y}$　　B. $\overline{X}+\overline{Y}$　　C. $\overline{X}+Y$　　D. $X+Y$

**试题（4）分析**

本题考查逻辑运算基础知识。

题中各逻辑式的真值表如下所示。

| X | Y | $X+\overline{X}Y$ | $X+\overline{Y}$ | $\overline{X}+\overline{Y}$ | $\overline{X}+Y$ | $X+Y$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |

**参考答案**

（4）D

**试题（5）**

在软件设计阶段，划分模块的原则是，一个模块的__（5）__。

（5）A．作用范围应该在其控制范围之内

B．控制范围应该在作用范围之内

C．作用范围与控制范围互不包含

D．作用范围与控制范围不受任何限制

**试题（5）分析**

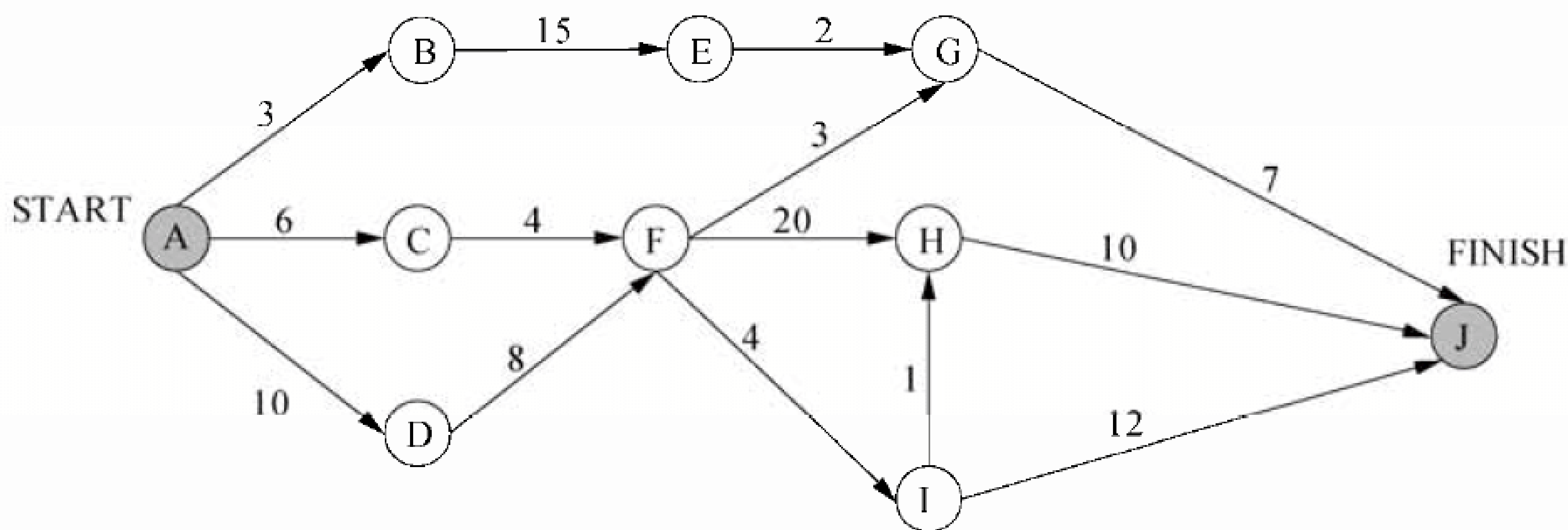
模块的作用范围定义为受该模块内一个判定影响的模块集合，模块的控制范围为模块本身以及所有直接或间接从属于该模块的模块集合。其作用范围应该在控制范围之内。

**参考答案**

（5）A

**试题（6）、（7）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑__（6）__在关键路径上，活动 FG 的松弛时间为__（7）__。




（6）A．B　　B．C　　C．D　　D．I

（7）A．19　　B．20　　C．21　　D．24

**试题（6）、（7）分析**

该活动图的关键路径为 ADFHJ，关键路径长度为 48 天，因此里程碑 D 在关键路径上，B、C 和 I 步骤关键路径上。活动 FG 的最早开始时间为第 19 天，最晚开始时间为第 39 天，因此松弛时间为 20 天。

**参考答案**

（6）C　　（7）B

**试题（8）**

设文件索引节点中有 8 个地址项，每个地址项大小为 4 字节，其中 5 个地址项为直接地址索引，2 个地址项是一级间接地址索引，1 个地址项是二级间接地址索引，磁盘索引块和磁盘数据块大小均为 1KB 字节。若要访问文件的逻辑块号分别为 5 和 518，则系

统应分别采用__（8）__。

（8）A．直接地址索引和一级间接地址索引

B．直接地址索引和二级间接地址索引

C．一级间接地址索引和二级间接地址索引

D．一级间接地址索引和一级间接地址索引

**试题（8）分析**

本题考查操作系统文件管理方面的基础知识。

根据题意，磁盘索引块为 1KB 字节，每个地址项大小为 4 字节，故每个磁盘索引块可存放 1024/4=256 个物理块地址。又因为文件索引节点中有 8 个地址项，其中 5 个地址项为直接地址索引，这意味着逻辑块号为 0～4 的为直接地址索引；2 个地址项是一级间接地址索引，这意味着第一个地址项指出的物理块中存放逻辑块号为 5～260 的物理块号，第一个地址项指出的物理块中存放逻辑块号为 261～516 的物理块号；1 个地址项是二级间接地址索引，该地址项指出的物理块存放了 256 个间接索引表的地址，这 256 个间接索引表存放逻辑块号为 517～66052 的物理块号。

经上分析不难得出，若要访问文件的逻辑块号分别为 5 和 518，则系统应分别采用一级间接地址索引和二级间接地址索引。

**参考答案**

（8）C

**试题（9）**

某企业有生产部和销售部，生产部负责生产产品并送入仓库，销售部从仓库取出产品销售。假设仓库可存放 *n* 件产品。用 PV 操作实现他们之间的同步过程如下图所示。

生产部
生产一件产品
P（S1）
P（S）
产品送仓库
V（S）
V（S2）

销售部
P（S2）
P（S）
从仓库取一件产品
V（S）
V（S1）
销售产品

图中信号量 S1 和 S2 为同步信号量，初值分别为 n 和 0；S 是一个互斥信号量，初值为__（9）__。

（9）A．0　　B．1　　C．n　　D．−1

**试题（9）分析**

本题考查 PV 操作方面的基本知识。

根据题意，可以通过设置三个信号量 S、$S_1$ 和 $S_2$，其中，S 是一个互斥信号量，初值为 1，因为仓库是一个互斥资源，所以将产品送仓库时需要执行进行 P（S）操作，当产品放入仓库后需要执行 V（S）操作。

**参考答案**

（9）B

**试题（10）**

M 软件公司的软件产品注册商标为 M，为确保公司在市场竞争中占据优势，对员工进行了保密约束。此情形下该公司不享有__（10）__。

（10）A．商业秘密权　B．著作权　C．专利权　D．商标权

**试题（10）分析**

本题考查知识产权基础知识。关于软件著作权的取得，《计算机软件保护条例》规定："软件著作权自软件开发完成之日起产生。"即软件著作权自软件开发完成之日起自动产生，不论整体还是局部，只要具备了软件的属性即产生软件著作权，既不要求履行任何形式的登记或注册手续，也无须在复制件上加注著作权标记，也不论其是否已经发表都依法享有软件著作权。软件开发经常是一项系统工程，一个软件可能会有很多模块，而每一个模块能够独立完成某一项功能。自该模块开发完成后就产生了著作权。软件公司享有商业秘密权。因为一项商业秘密受到法律保护的依据，必须具备构成商业秘密的三个条件，即不为公众所知悉、具有实用性、采取了保密措施。商业秘密权保护软件是以软件中是否包含着"商业秘密"为必要条件的。该软件公司组织开发的应用软件具有商业秘密的特征，即包含着他人不能知道到的技术秘密；具有实用性，能为软件公司带来经济效益；对职工进行了保密的约束，在客观上已经采取相应的保密措施。所以软件公司享有商业秘密权。商标权、专利权不能自动取得，申请人必须履行商标法、专利法规定的申请手续，向国家行政部门提交必要的申请文件，申请获准后即可取得相应权利。获准注册的商标通常称为注册商标。

**参考答案**

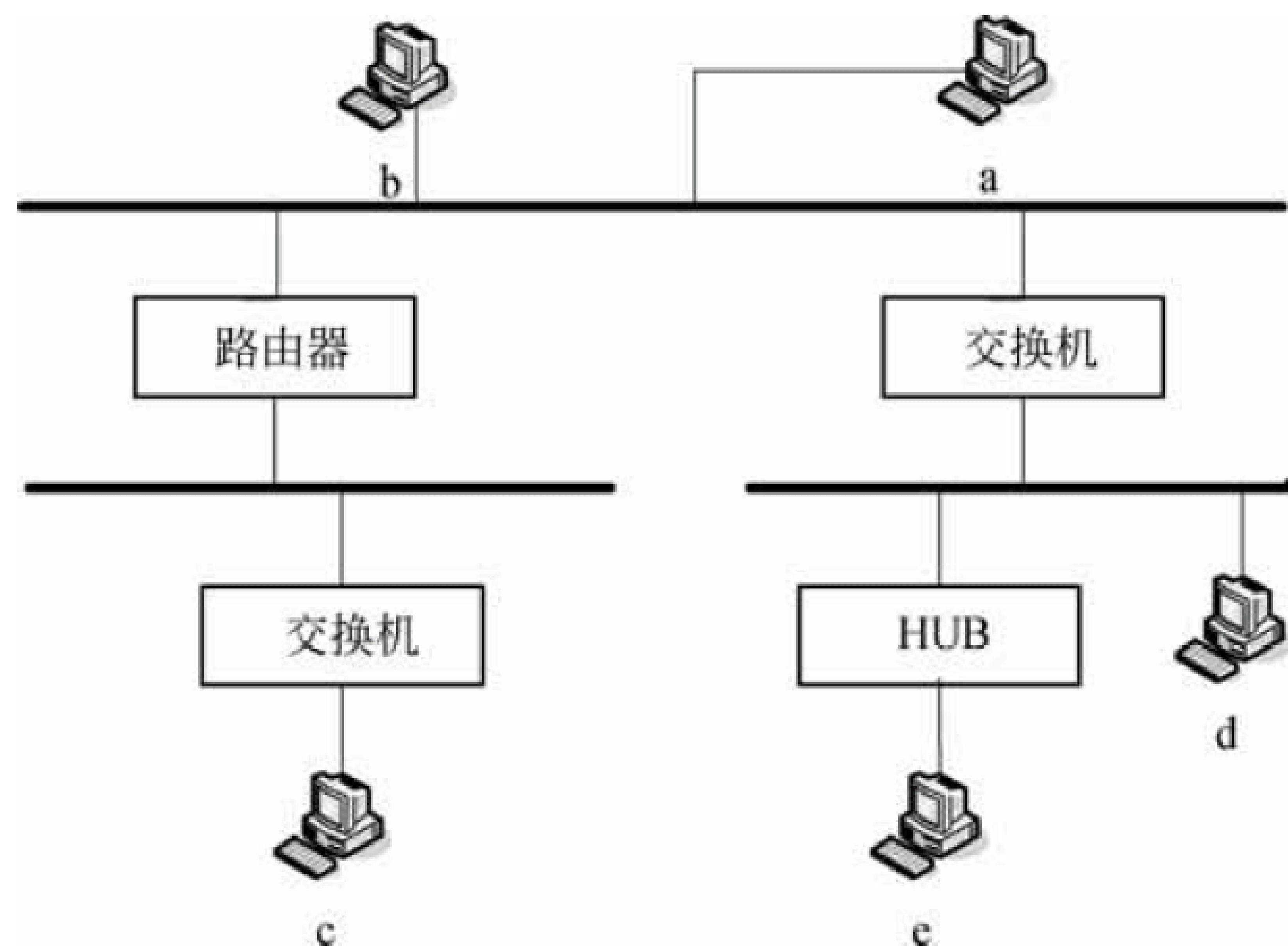
（10）C

**试题（11）、（12）**

下面的地址中，属于全局广播地址的是__（11）__。在下面的网络中，IP 全局广播分组不能通过的通路是__（12）__。

（11）A．172.17.255.255　B．0.255.255.255
C．255.255.255.255　D．10.255.255.255

（12）A．a 和 b 之间的通路　B．a 和 c 之间的通路
C．b 和 d 之间的通路　D．b 和 e 之间的通路




**试题（11）、（12）分析**

IP 地址可以划分为“网络地址”和“主机地址”两部分。主机地址部分全为“0”地址称为网络地址，例如 129.45.0.0 就是指一个 B 类网络地址。主机地址部分全为“1”的地址称为广播地址，例如 129.45.255.255 就是一个 B 类广播地址，这种地址也称为定向广播地址，意味着网络 129.45.0.0 中的主机都可以接收这个数据报。所有字节为全“1”的地址 255.255.255.255 是全局广播地址，理论上，以这种地址为目标地址的全局广播分组可以传播到任何网络中去，但是为了避免不必要的通信干扰，一般路由器都会阻止这种分组进入本地网络，所以全局广播分组一般不能通过路由器进行扩散，也就是说，路由器可以把整个互联网络分成互相区分的许多子网。

**参考答案**

（11）C　（12）B

**试题（13）**

下面用于表示帧中继虚电路标识符的是（13）。

（13）A．CIR　B．LMI　C．DLCI　D．VPI

**试题（13）分析**

帧中继协议 LAP-D（Q.921）的帧格式如下图所示。帧头和帧尾都是编码为“01111110”的帧标志字段，信息字段长度可变，1600 是默认的最大长度。帧效验序列 FCS 与 HDLC 的相同。EA 为地址扩展比特，EA 为 0 时表示地址向后扩展一个字节，EA 为 1 时表示最后一个字节。C/R 是命令/响应比特，协议本身不使用这个比特，用户可以用这个比特区分不同的帧。FECN 是向前拥塞比特，若网络置该位为 1，则表示在帧的传送方向上出现了拥塞，BECN 是向后拥塞比特，若网络置该位为 1，则表示在与帧传送相反的方向上出现了拥塞。DE 是优先丢弃比特，当网络发生拥塞时，DE 置位的帧被优先丢弃。最后，DLCI 表示数据链路连接标识符。

| 01111110 | 地址 | 信息 | FCS | 01111110 |
|---|---|---|---|---|
| 1 | 2~4 | 长度可变 | 2 | 1 |

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| DLCI（高位） | | | | | | C/R | EA=0 |
| DLCI（低位） | | | | FECN | BECN | DE | EA=1 |

**参考答案**

（13）C

**试题（14）**

下面关于 RS-232-C 标准的描述中，正确的是<u>（14）</u>。

（14）A．可以实现长距离远程通信

B．可以使用 9 针或 25 针 D 型连接器

C．必须采用 24 根线的电缆进行连接

D．通常用于连接并行打印机

**试题（14）分析**

RS-232-C 是美国电子工业协会制定的串行接口标准，其机械特性规定可以使用 9 针或 25 针的 D 型连接器。功能特性采用 V.24 建议，如果只采用主通道进行双工通信，仅需少数几根线（例如 3 根或 9 根）就可以了。由于驱动器允许有 2500pF 的电容负载，所以通信距离会受到限制，例如采用 150pF/m 的电缆时，最大通信距离为 15m。另外，由于这个标准采用单端信号传送，共地噪声和共模干扰也限制了信号传送的距离，一般状况下，通信距离不超过 20m。

**参考答案**

（14）B

**试题（15）**

设信道带宽为 4000Hz，采用 PCM 编码，采样周期为 125μs，每个样本量化为 128 个等级，则信道的数据速率为<u>（15）</u>。

（15）A．10kb/s　B．16kb/s　C．56kb/s　D．64kb/s

**试题（15）分析**

PCM 通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组。采样的频率决定了可恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍。所以对带宽为 4000Hz 的信号的采样频率必须大于 8000Hz，即 125μs。量化为 128 个等级，即用 7 位二进制编码来表示一个采样值，这样，7×8000=56kb/s。

**参考答案**

（15）C

**试题（16）、（17）**

在异步通信中，每个字符包含1位起始位、7位数据位、1位奇偶位和1位终止位，每秒钟传送200个字符，采用DPSK调制，则码元速率为__（16）__，有效数据速率为__（17）__。

（16）A．200波特　B．500波特　C．1000波特　D．2000波特

（17）A．200b/s　B．1000b/s　C．1400b/s　D．2000b/s

**试题（16）、（17）分析**

由于每个字符包含1位起始位、7位数据位、1位奇偶位和1位终止位，总共10位，每秒钟传送200个字符，即波特率为10×200=2000波特。而有效数据速率为7×200=1400b/s。

**参考答案**

（16）D　（17）C

**试题（18）**

以下关于ICMP协议的说法中，正确的是__（18）__。

（18）A．由MAC地址求对应的IP地址

B．在公网IP地址与私网IP地址之间进行转换

C．向源主机发送传输错误警告

D．向主机分配动态IP地址

**试题（18）分析**

在TCP/IP协议簇中，ICMP协议的作用是提供网络层通信过程的差错控制和告警，以及网络邻居发现等功能，例如向源主机发送目标不可到达警告、获取默认路由器的地址等。

**参考答案**

（18）C

**试题（19）**

以下关于RARP协议的说法中，正确的是__（19）__。

（19）A．RARP协议根据主机IP地址查询对应的MAC地址

B．RARP协议用于对IP协议进行差错控制

C．RARP协议根据MAC地址求主机对应的IP地址

D．RARP协议根据交换的路由信息动态改变路由表

**试题（19）分析**

ARP协议根据目标的IP地址获取目标的MAC地址，而RARP协议根据本地主机的MAC地址请求对应的IP地址，这个协议主要用在无盘工作站中。

**参考答案**

（19）C

**试题（20）**

所谓“代理 ARP”是指由__（20）__假装目标主机回答源主机的 ARP 请求。

（20）A．离源主机最近的交换机　　B．离源主机最近的路由器

C．离目标主机最近的交换机　　D．离目标主机最近的路由器

**试题（20）分析**

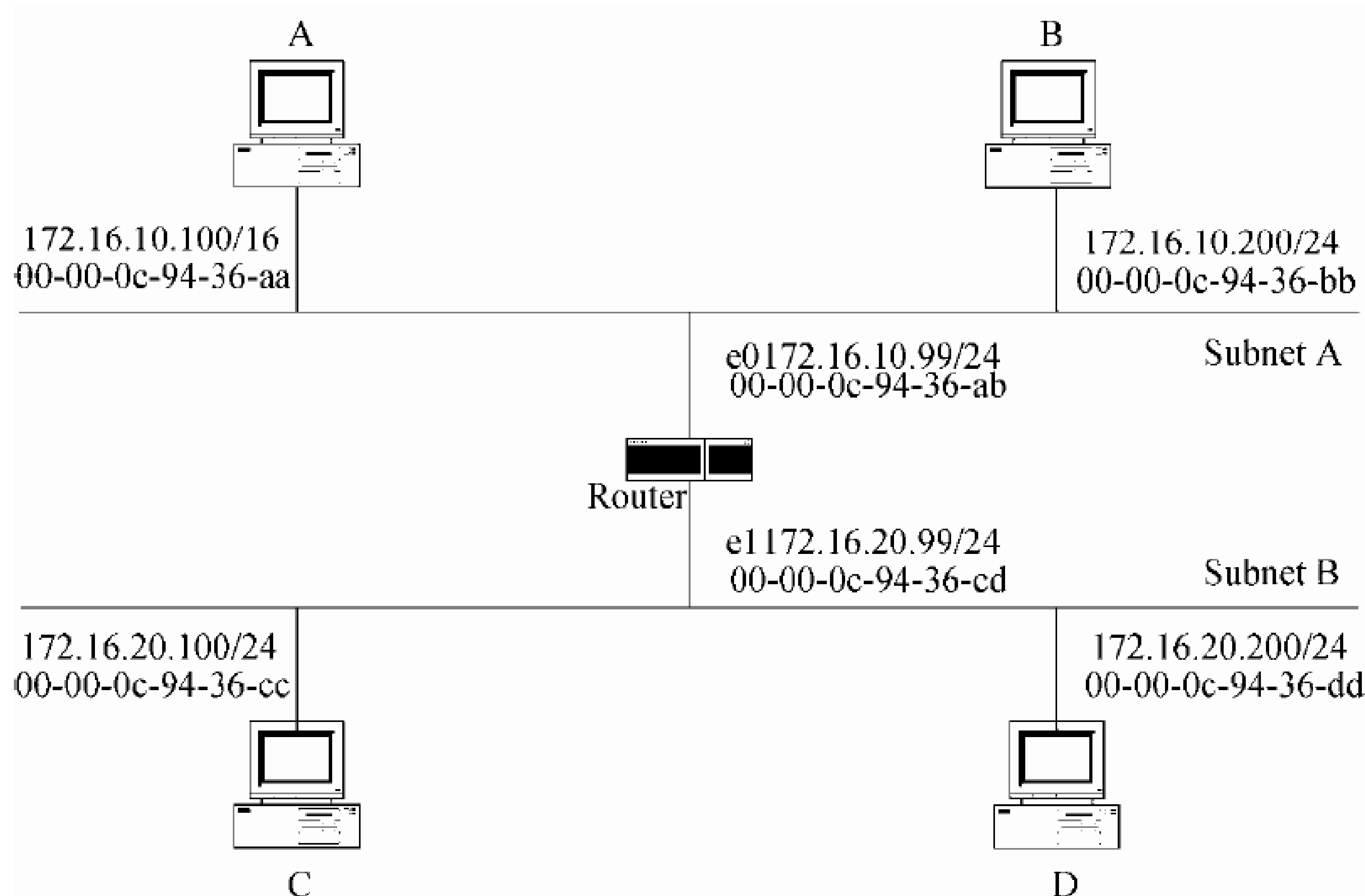
当两个主机通过 Internet 通信时，如果发送方主机不知道目标主机的 MAC 地址，就要广播一个 ARP 请求分组，这种分组的作用是由目标主机的 IP 地址求对应的 MAC 地址。收到这种请求分组的主机用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址，若不相符则不予回答。

代理 ARP 如下图所示，设子网 A 上的主机 A（172.16.10.100）需要与子网 B 上的主机 D（172.16.20.200）通信。当主机 A 需要与它直接连接的设备通信时，它就向目标发送一个 ARP 请求。

主机 A 在子网 A 上广播的 ARP 请求分组是：

| 发送者的 MAC 地址 | 发送者的 IP 地址 | 目标的 MAC 地址 | 目标的 IP 地址 |
|---|---|---|---|
| 00-00-0c-94-36-aa | 172.16.10.100 | 00-00-00-00-00-00 | 172.16.20.200 |

这个请求的含义是要求主机 D（172.16.20.200）回答它的 MAC 地址。ARP 请求分组被包装在以太帧中，其源地址是 A 的 MAC 地址，而目标地址是广播地址（FFFF.FFFF.FFFF）。由于路由器不转发广播帧，所以这个 ARP 请求只能在子网 A 中传播，而到不了主机 D。



如果路由器知道目标地址（172.16.20.200）在另外一个子网中，它就以自己的 MAC 地址回答主机 A，路由器发送的应答分组是：

| 发送者的 MAC 地址 | 发送者的 IP 地址 | 目标的 MAC 地址 | 目标的 IP 地址 |
|---|---|---|---|
| 00-00-0c-94-36-ab | 172.16.20.200 | 00-00-0c-94-36-aa | 172.16.10.100 |

这个应答分组包装在以太帧中，以路由器的 MAC 地址为源地址，以主机 A 的 MAC 地址为目标地址，ARP 应答帧是单播传送的。在接收到 ARP 应答后，主机 A 就更新它的 ARP 表：

| IP Address | MAC Address |
|---|---|
| 172.16.20.200 | 00-00-0c-94-36-ab |

此后主机 A 就把所有发送给主机 D（172.16.20.200）的分组发送给 MAC 地址为 00-00-0c-94-36-ab 的主机，这就是路由器的网卡地址。

通过这种方式，子网 A 中的 ARP 映像表都把路由器的 MAC 地址当作子网 B 中主机的 MAC 地址。例如主机 A 的 ARP 映像表如下所示：

| IP Address | MAC Address |
|---|---|
| 172.16.20.200 | 00-00-0c-94-36-ab |
| 172.16.20.100 | 00-00-0c-94-36-ab |
| 172.16.10.99 | 00-00-0c-94-36-ab |
| 172.16.10.200 | 00-00-0c-94-36-bb |

多个 IP 地址被映像到一个 MAC 地址这一事实正是代理 ARP 的标志。

**参考答案**

（20）B

**试题（21）**

在距离矢量路由协议中，每一个路由器接收的路由信息来源于__（21）__。

（21）A．网络中的每一个路由器　　B．它的邻居路由器

C．主机中存储的一个路由总表　　D．距离不超过两个跳步的其他路由器

**试题（21）分析**

ARPAnet 最初采用了距离矢量路由协议 RIP，RIPv1 使用本地广播地址 255.255.255.255 发布路由信息，默认的路由更新周期为 30 秒，持有时间（Hold-Down Time）为 180 秒。也就是说，RIP 路由器每 30 秒向所有邻居发送一次路由更新报文，如果在 180 秒之内没有从某个邻居接收到路由更新报文，则认为该邻居不存在了。收到邻居发来的距离矢量后，路由器采用 Ford-Fulkerson 算法重新计算路由表。

**参考答案**

（21）B

**试题（22）、（23）**

在 BGP4 协议中，__（22）__报文建立两个路由器之间的邻居关系，__（23）__报文给

出了新的路由信息。

（22）A. 打开（open）　B. 更新（update）
　　C. 保持活动（keepalive）　D. 通告（notification）

（23）A. 打开（open）　B. 更新（update）
　　C. 保持活动（keepalive）　D. 通告（notification）

**试题（22）、（23）分析**

外部网关协议 BGP 4 广泛地应用于不同 ISP 的网络之间，成为事实上的 Internet 外部路由协议标准。BGP 4 是一种动态路由发现协议，支持无类别域间路由 CIDR。BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 的 4 种报文表示在下表中。

| 报 文 类 型 | 功 能 描 述 |
|---|---|
| 打开（Open） | 建立邻居关系 |
| 更新（Update） | 发送新的路由信息 |
| 保持活动状态（Keepalive） | 对 Open 的应答/周期性地确认邻居关系 |
| 通告（Notification） | 报告检测到的错误 |

在 BGP 中用上述 4 种报文可实现以下 3 个功能过程：

- 建立邻居关系。建立邻居关系的过程是由一个路由器发送 Open 报文，另一个路由器若愿意接受请求则以 Keepalive 报文应答。Open 报文中包含发送者的 IP 地址及其所属自治系统的标识，另外还有一个保持时间参数，即定期交换信息的时间间隔。接收者把 Open 报文中的保持时间与自己的保持时间计数器比较，选取其中的较小者，这就是一次交换信息保持有效的最长时间。建立邻居关系的一对路由器以选定的周期交换路由信息。
- 邻居可到达性。这个过程维护邻居关系的有效性，通过周期性地互相发送 Keepalive 报文，双方都知道对方的活动状态。
- 网络可到达性。每个路由器维护一个数据库，记录着它可到达的所有子网。当情况有变化时用更新报文把最新消息及时地传送给其他 BGP 路由器。Update 报文包含两类信息：一类是要作废的路由器列表，另一类是新增路由的属性信息。

**参考答案**

（22）A　（23）B

**试题（24）**

在 OSPF 协议中，链路状态算法用于<u>（24）</u>。

（24）A. 生成链路状态数据库　B. 计算路由表
　　C. 产生链路状态公告　D. 计算发送路由信息的组播树

**试题（24）分析**

OSPF 是一种链路状态协议，用于在自治系统内部的路由器之间交换路由信息。OSPF 路由器发布链路状态公告，报告本地网络各个链路的状态信息。路由器收到的链路状态信息保存在本地的链路状态数据库中，这些数据可用于构造网络拓扑结构图。路由器使用 Dijkstra 的最短通路优先算法（Shortest Path First，SPF）根据网络拓扑结构图计算到达各个目标的最佳路由，生成新的路由表。

**参考答案**

（24）B

**试题（25）**

以下关于两种路由协议的叙述中，错误的是 （25） 。

（25）A．链路状态协议在网络拓扑发生变化时发布路由信息

B．距离矢量协议是周期性地发布路由信息

C．链路状态协议的所有路由器都发布路由信息

D．距离矢量协议是广播路由信息

**试题（25）分析**

链路状态协议与距离矢量协议发布路由信息的时机不同，链路状态协议是在网络拓扑发生变化时才发布路由信息；而距离矢量协议是周期性地发布路由信息。链路状态协议使用了分层的网络结构，在广播网络或 NBMA 网络构成的区域中，OSPF 协议要选举一个指定路由器（DR），由 DR 代表这个网络向外界发布路由信息，从而减小了链路状态公告的传播范围，同时也减小了网络拓扑变化时影响所有路由器的可能性；与之相反，距离矢量网络是扁平结构，所有路由器都在发布路由信息，并且网络某一部分出现的变化会影响到网络中的所有路由器。链路状态协议使用组播来共享路由信息，并且发布的是增量式的更新消息，这使得网络带宽的利用率和资源消耗率得到改善；而距离矢量协议 RIP 是每隔 30 秒向所有邻居广播路由更新报文。链路状态协议支持无类别域间路由和路由汇聚功能，通过 CIDR 技术使得发布的路由信息减少，也使得链路状态数据库减小，从而减少了所需要的 CPU 周期，也减少了路由器中的存储需求；距离矢量协议 RIPv1 是有类别的协议，不支持 CIDR 技术。链路状态协议使用 SPF 算法计算最短通路，不会在路由表中出现环路，而这是距离矢量路由协议难以处理问题，必须采用水平分割、反向路由毒化或触发更新等特别方法来加快路由收敛，防止路由环路的形成。

**参考答案**

（25）C

**试题（26）、（27）**

下面的 D 类地址中，可用于本地子网作为组播地址分配的是 （26） 。一个组播组包含 4 个成员，当组播服务器发送信息时需要发出 （27） 个分组。

（26）A．224.0.0.1　　B．224.0.1.1　　C．234.0.0.1　　D．239.0.1.1

（27）A．1　　B．2　　C．3　　D．4

**试题（26）、（27）分析**

组播技术用于向一组目标发送同样的分组，每一个组播组被指定了一个 D 类地址作为组标识符，组播源利用组地址作为目标地址来发送分组。组播成员向网络发出通知，声明它期望加入的组的地址。IGMP 协议用于支持接收者加入或离开组播组。一旦有接收者加入了一个组，就要为这个组在网络中构建一个组播分布树，用于生成和维护组播树的协议有许多种，例如独立组播协议 PIM 等。在 IP 组播模式下，组播源无须知道所有的组成员，组播树的构建是由接收者驱动的，是由最接近接收者的网络结点完成的，这样建立的组播树可以扩展到很大的范围。有人形容 IP 组播模型是：你在一端注入一个分组，网络正好可以把这个分组提交给所有需要的接收者。

IPv4 的 D 类地址是组播地址，用作一个组的标识符，其地址范围是 224.0.0.0～239.255.255.255。按照约定，D 类地址被划分为 3 类：

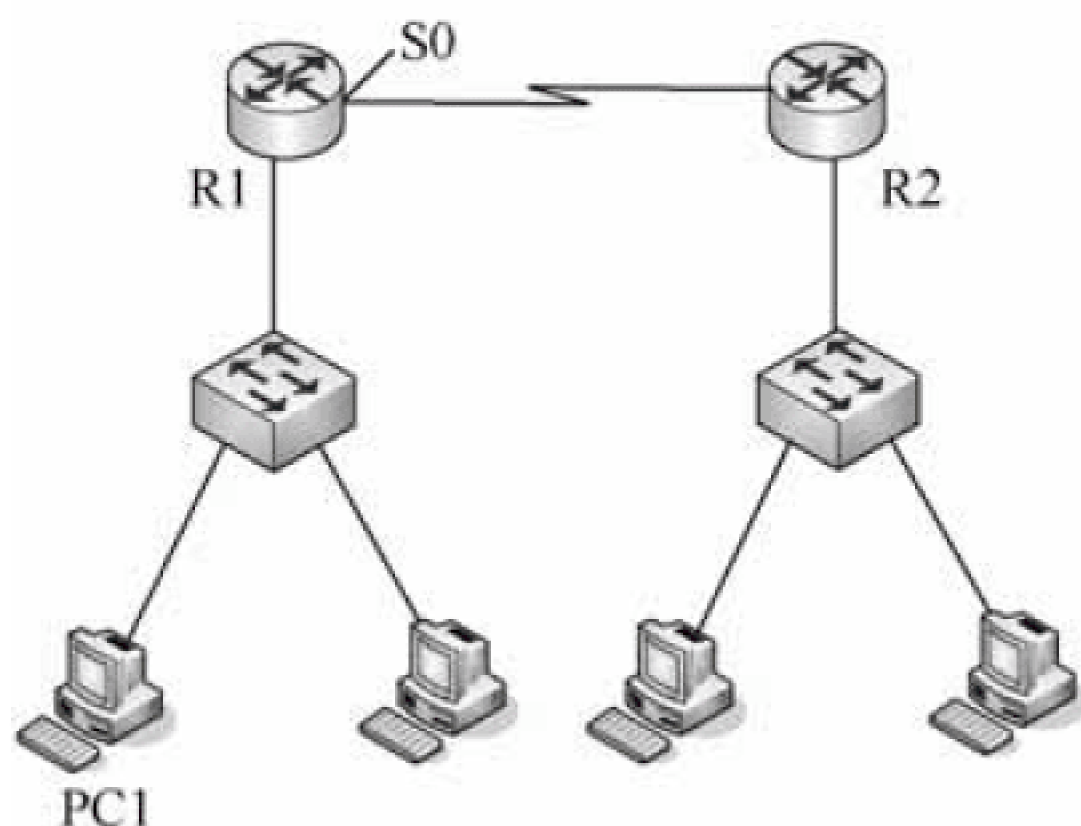
- 224.0.0.0～224.0.0.255：保留地址，用于路由协议或其他下层拓扑发现协议以及维护管理协议等，例如 224.0.0.1 代表本地子网中的所有主机，224.0.0.2 代表本地子网中的所有路由器，224.0.0.5 代表所有 OSPF 路由器，224.0.0.9 代表所有 RIP 2 路由器，224.0.0.12 代表 DHCP 服务器或中继代理，224.0.0.13 代表所有支持 PIM 的路由器等。
- 224.0.1.0～238.255.255.255：用于全球范围的组播地址分配，可以把这个范围的 D 类地址动态地分配给一个组播组，当一个组播会话停止时，其地址被回收，以后还可以分配给新出现的组播组。
- 239.0.0.0～239.255.255.255：在管理权限范围内使用的组播地址，限制了组播的范围，可以在本地子网中作为组播地址使用。

**参考答案**

（26）D　（27）A

**试题（28）～（31）**

某网络拓扑结构如下图所示。



在路由器 R2 上采用命令（28）得到如下所示结果。

```
Router>
…
R    192.168.0.0/24 [120/1] via 202.117.112.1, 00:00:11, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
  202.117.112.0/30 is subnetted, 1 subnets
C    202.117.112.0 is directly connected, Serial2/0
Router>
```

则 PC1 可能的 IP 地址为（29），路由器 R1 的 S0 口的 IP 地址为（30），路由器 R1 和 R2 之间采用的路由协议为（31）。

（28）A. netstat -r　B. show ip route　C. ip routing　D. route print

（29）A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2

（30）A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2

（31）A. OSPF　B. RIP　C. BGP　D. IGRP

**试题（28）～（31）分析**

本题考查路由器配置、路由相关基础知识。

在路由器上查看路由的命令为 show ip route。

由题干显示的 R2 路由信息可知，网络 192.168.1.0/24 直连快速以太口 0/0，网络 202.117.112.0/30 直连串口 2/0，网络 192.168.0.0/24 经串口 2 路由可达。由此可判断 PC1 所在网络为 192.168.0.0/24，路由器 R1 的 S0 口和 202.117.112.1 在一个子网，故 PC1 可能的 IP 地址为 192.168.0.1，路由器 R1 的 S0 口的 IP 地址为 202.117.112.2。

又由网络 192.168.0.0/24 经串口 2 路由采用协议的标志为“R”可知，路由器 R1 和 R2 之间采用的路由协议为 RIP。

**参考答案**

（28）B　（29）A　（30）D　（31）B

**试题（32）**

DNS 服务器中提供了多种资源记录，其中（32）定义了区域的授权服务器。

（32）A. SOA　B. NS　C. PTR　D. MX

**试题（32）分析**

本题考查 DNS 服务器资源记录相关基础知识。

资源记录分为许多不同的类型，常用的是（参见下表）：

- SOA（Start Of Authoritative）：开始授权记录是区域文件的第一条记录，指明区域的主服务器，指明区域管理员的邮件地址，并给出区域复制的有关信息。
- 序列号：当区域文件改变时，序列号要增加，辅助服务器把自己的序列号与主服务器的序列号比较，以确定是否需要更新数据。

- 刷新间隔：辅助服务器更新数据的时间间隔（秒）。
- 重试间隔：当辅助服务器不能连接主服务器进行更新时，必须每隔一定时间间隔（秒）重新试图连接。
- 有效期：如果辅助服务器不能更新自己的区域文件，超过有效期（秒）后就不再提供查询服务。
- 生命期（TTL）：资源记录在其他名字服务器缓存中保存的最少有效时间（秒）。
- A（Address）：地址记录表示主机名到 IP 地址的映像。
- PTR（Pointer）：指针记录是 IP 地址到主机名的映射。
- NS（Name Server）：给出区域的授权服务器。
- MX（Mail eXchanger）：定义了区域的邮件服务器及其优先级（搜索顺序）。
- CNAME：为正式主机名（canonical name）定义了一个别名（alias）。

| 记录类型 | 说　明 | 示　例 |
|---|---|---|
| 开始授权（SOA） | 指明区域主服务器(primary nameserver)<br>指明区域管理员的邮件地址，及区域复制信息：<br>序列号<br>刷新间隔<br>重试间隔<br>有效期<br>TTL | 区域 microsoft.com<br>的主服务器为 ns1.microsoft.com<br>2003080800　;serial number<br>172800　;refresh=2d<br>900　;retry=15m<br>1209600　;expire=2w<br>3600　;default TTL=1h |
| 地址（A） | 最常用的资源记录<br>把主机名解析为 IP 地址 | compuer1.microsoft.com 被解析为 10.1.1.4 |
| 指针（PTR） | 用于反向查询的资源记录<br>把 IP 地址解析为主机名 | 10.1.1.4 被解析为 compuer1.microsoft.com |
| 名字服务器（NS） | 为一个域指定了授权服务器<br>该域的所有子域也被委派给这个服务器 | 域 microsoft.com 的授权服务器为 ns2.microsoft.com |
| 邮件服务器（MX） | 指明区域的 SMTP 服务器 | 区域 microsoft.com 的邮件服务器为 mail.microsoft.com |
| 别名（CNAME） | 指定主机的别名<br>把主机名解析为另一个主机名 | www.microsoft.com 的别名为 webserver12.microsoft.com |

**参考答案**

（32）　B

**试题（33）**

某主机本地连接属性如下图所示，下列说法中错误的是__（33）__。




（33）A．IP 地址是采用 DHCP 服务自动分配的

B．DHCP 服务器的网卡物理地址为 00-1D-7D-39-62-3E

C．DNS 服务器地址可手动设置

D．主机使用该地址的最大租约期为 7 天

**试题（33）分析**

本题考查 DHCP 服务器配置相关知识。

从该主机的本地连接属性可以看出：该主机的 MAC 地址为 00-1D-7D-39-62-3E，IP 地址是采用 DHCP 服务自动分配的，租约期为 7 天。在选用 DHCP 自动分配 IP 地址时，可以手工设置 DNS 服务器地址。

**参考答案**

（33）B

**试题（34）、（35）**

Linux 系统中，DHCP 服务的主配置文件是__（34）__，保存客户端租约信息的文件是__（35）__。

（34）A．dhcpd.leases　　B．dhcpd.conf　　C．xinetd.conf　　D．lease.conf

（35）A．dhcpd.leases　　B．dhcpd.conf　　C．xinetd.conf　　D．lease.conf

**试题（34）、（35）分析**

本题考查 Linux 系统下 DHCP 服务器配置的基础知识。

在 Linux 系统中，DHCP 服务由 dhcpd 提供，dhcpd 的配置文件是/etc/dhcpd.conf，dhcpd 中用于保存客户端租约信息的文件是/var/lib/dhcp/dhcpd.leases。

**参考答案**

（34）B　（35）A

**试题（36）**

在 Windows Server 2003 操作系统中，WWW 服务包含在__（36）__组件下。

（36）A．DNS　　B．DHCP　　C．FTP　　D．IIS

**试题（36）分析**

本题考查在 Windows Server 2003 操作系统下有关网络服务组件的基础知识。

在 Windows Server 2003 操作系统下，虽然也包含 DNS、DHCP 服务，但 WWW、FTP 是包含在 IIS（Internet Information Services）服务下的。

**参考答案**

（36）D

**试题（37）**

DNS 正向搜索区的功能是将域名解析为 IP 地址，Windows XP 系统中用于测试该功能的命令是__（37）__。

（37）A．nslookup　　B．arp　　C．netstat　　D．query

**试题（37）分析**

本题考查在 Windows XP 操作系统下,常用的网络有关测试命令使用基础知识。

query：显示与终端服务器上运行的进程、用户会话等有关信息。

netstat：可以使用户了解到自己的主机是怎样与Internet相连接的，这有助于用户了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，如网络连接、路由表和网络接口等信息，也可以让用户得知目前总共有哪些网络连接正在运行。

arp：显示和修改地址解析协议缓存中的项目，ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。

nslookup：显示可用来诊断域名系统（DNS）基础结构的信息。

**参考答案**

（37）A

**试题（38）**

在 Windows 环境下，DHCP 客户端可以使用__（38）__命令重新获得 IP 地址，这时客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包来请求重新租用 IP 地址。

（38）A．ipconfig/renew　　B．ipconfig/reload

C．ipconfig/release　　D．ipconfig/reset

**试题（38）分析**

本题考查在 Windows 操作系统下，DHCP 网络服务启动后，手动获取 IP 地址的知识。

ipconfig 命令的参数/renew：重新获得 IP 地址，符合本题的要求。

ipconfig 命令的参数/release：所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。

/reload 和/reset 是两个干扰项，ipconfig 不支持这两个参数。

**参考答案**

（38）A

**试题（39）**

匿名 FTP 访问通常使用__（39）__作为用户名。

（39）A. guest　　B. ip 地址　　C. administrator　　D. anonymous

**试题（39）分析**

本题考查有关 FTP 服务的管理基础知识，匿名用户的用户名称。

一般情况下，匿名用户的英语名称就是 anonymous，guest 是来宾用户，administrator 是超级用户，ip 地址是干扰项，不能使用 ip 地址作为 FTP 访问用户名。

**参考答案**

（39）D

**试题（40）**

下列不属于电子邮件协议的是__（40）__。

（40）A. POP3　　B. SMTP　　C. SNMP　　D. IMAP4

**试题（40）分析**

本题考查常用的电子邮件有关协议的基础知识。

在TCP/IP 协议簇中，包含了常用的电子邮件协议 SMTP、POP3、IMAP4，而 SNMP 是简单网络管理协议（Simple Network Management Protocol）。

**参考答案**

（40）C

**试题（41）**

下列安全协议中，与 TLS 功能相似的协议是__（41）__。

（41）A. PGP　　B. SSL　　C. HTTPS　　D. IPSec

**试题（41）分析**

本题考查安全协议方面的基础知识。

SSL（Secure Socket Layer，安全套接层）是 Netscape 于 1994 年开发的传输层安全协议，用于实现 Web 安全通信。1996 年发布的 SSL 3.0 协议草案已经成为一个事实上的 Web 安全标准。

TLS（Transport Layer Security，传输层安全协议）是 IETF 制定的协议，它建立在 SSL 3.0 协议规范之上，是 SSL 3.0 的后续版本。

**参考答案**

（41）B

**试题（42）、（43）**

用户 B 收到用户 A 带数字签名的消息 M，为了验证 M 的真实性，首先需要从 CA 获取用户 A 的数字证书，并利用__（42）__验证该证书的真伪，然后利用__（43）__验证 M

的真实性。

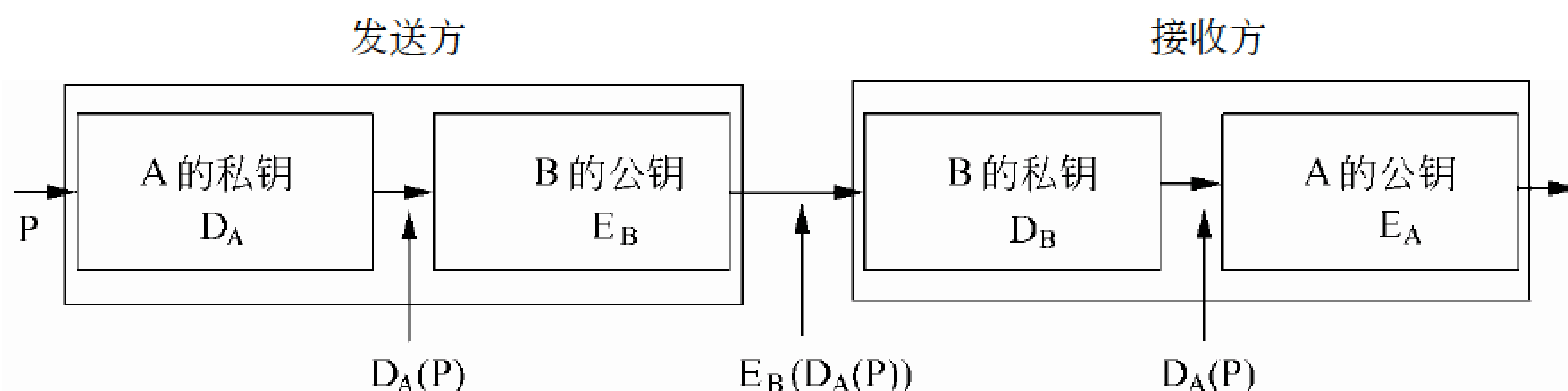
（42）A. CA 的公钥　　B. B 的私钥　　C. A 的公钥　　D. B 的公钥

（43）A. CA 的公钥　　B. B 的私钥　　C. A 的公钥　　D. B 的公钥

**试题（42）、（43）分析**

本题考查数字签名和数字证书方面的知识。

基于公钥的数字签名系统如下图所示：A 为了向 B 发送消息 P，A 用字节的私钥对 P 签名后再用 B 的公钥对签名后的数据加密，B 收到消息后先用 B 的私钥解密后在用 A 的公钥认证 A 的签名以及消息的真伪。




用户 B 收到用户 A 带数字签名的消息 M，为了验证 M 的真实性，首先需要从 CA 获取用户 A 的数字证书，验证证书的真伪需要用 CA 的公钥验证 CA 的签名，验证 M 的真实性需要用用户 A 的公钥验证用户 A 的签名。

**参考答案**

（42）A　　（43）C

**试题（44）**

3DES 是一种__（44）__算法。

（44）A. 共享密钥　　B. 公开密钥　　C. 报文摘要　　D. 访问控制

**试题（44）分析**

本题考查加密方面的基础知识。

3DES 是 DES 的改进算法，它使用两把密钥对报文作三次 DES 加密，效果相当于将 DES 密钥的长度加倍了，克服了 DES 密钥长度较短的缺点。

3DES 跟 DES 一样，是一种共享密钥加密算法。

**参考答案**

（44）A

**试题（45）**

IPSec 中安全关联（Security Associations）三元组是__（45）__。

（45）A. <安全参数索引 SPI，目标 IP 地址，安全协议>

B. <安全参数索引 SPI，源 IP 地址，数字证书>

C. <安全参数索引 SPI，目标 IP 地址，数字证书>

D. <安全参数索引 SPI，源 IP 地址，安全协议>

**试题（45）分析**

本题考查 IPSec 方面的基础知识。

安全关联（Security Association，简称 SA）是 IPSec 的基础，是两个应用 IPSec 系统（主机、路由器）间的一个单向逻辑连接，是安全策略的具体化和实例化，它提供了保护通信的具体细节。一个 SA 由一个三元组唯一标识，该三元组是：一个安全参数索引（SPI）、一个 IP 目的地址和一个安全协议（AH 或 ESP）标识符。

**参考答案**

（45）A

**试题（46）**

在 SNMP 协议中，当代理收到一个 GET 请求时，如果有一个值不可或不能提供，则返回__（46）__。

（46）A．该实例的下个值　　B．该实例的上个值
　　C．空值　　D．错误信息

**试题（46）分析**

本题考查 SNMP 协议中检索简单对象的相关基础知识。

在 SNMP 协议中检索简单对象时，当代理收到一个 GET 请求时：如果能检索到所有的对象实例，则返回请求的每个值；如果有一个值不可或者不能提供，则返回该实例的下一个值。

**参考答案**

（46）A

**试题（47）**

SNMP 网络管理中，一个代理可以由__（47）__管理站管理。

（47）A．0 个　　B．1 个　　C．2 个　　D．多个

**试题（47）分析**

本题考查 SNMP 协议体系架构中的相关基础知识。

SNMP 要求所有的代理设备和管理站都必须实现 TCP/IP 协议。对于不支持 TCP/IP 的设备不能直接用 SNMP 进行管理。为此提出了委托代理的概念。一个委托代理设备可以管理若干台非 TCP/IP 设备，并代表这些设备接收管理站的查询，同时与某些管理站建立团体关系。

**参考答案**

（47）D

**试题（48）**

在 Windows 命令行下执行__（48）__命令出现下图的效果。

```
Tracing route to microsoft [157.54.1.196] over a maximum of 30 hops:
0   172.16.87.35
1   172.16.87.218
2   192.168.52.1
3   192.168.80.1
4   157.54.247.14
5   157.54.1.196

Computing statistics for 125 seconds...Source to Here   This
Node/Link

Hop  RTT     Lost/Sent = Pct  Lost/Sent = Pct  Address
0                                              172.16.87.35
                                 0/ 100 =  0%   |
1    41ms     0/ 100 =  0%       0/ 100 =  0%  172.16.87.218
                                13/ 100 = 13%   |
2    22ms    16/ 100 = 16%       3/ 100 =  3%  192.168.52.1
                                 0/ 100 =  0%   |
3    24ms    13/ 100 = 13%       0/ 100 =  0%  192.168.80.1
                                 0/ 100 =  0%   |
4    21ms    14/ 100 = 14%       1/ 100 =  1%  157.54.247.14
                                 0/ 100 =  0%   |
5    24ms    13/ 100 = 13%       0/ 100 =  0%  157.54.1.196

Trace complete.
```

（48）A．pathping -n microsoft　　B．tracert -d microsoft

C．nslookup microsoft　　D．arp -a

**试题（48）分析**

本题考查网络管理命令的使用。

pathping 是一个基于 TCP/IP 的命令行工具，它可以反映出数据包从源主机到目标主机所经过的路径、网络延时以及丢包率，帮助我们解决网络问题。它使用 ICMP 回应信息来分析网络连通情况。pathping 发送回应信息到源地址与目标地址之间的所有路由器。

-n 参数可以阻止 pathping 试图将中间路由器的 IP 地址解析为各自的名称。这有可能加快 pathping 的结果显示。

tracert 是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。

nslookup 是一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。

arp 命令用来显示和修改 arp 缓存中的值。

**参考答案**

（48）A

**试题（49）**

在 Windows 系统中监听发送给 NT 主机的陷入报文的程序是＿（49）＿。

（49）A．snmp.exe　　B．mspaint.com　　C．notepad.exe　　D．snmptrap.exe

**试题（49）分析**

本题考查 Windows SNMP 服务的基本概念。

Windows NT 的 SNMP 的服务包括两个应用程序。一个是 SNMP 代理服务程序 snmp.exe，另一个是 SNMP 陷入服务程序 snmptrap.exe。snmp.exe 接收 SNMP 请求报文，根据要求发送响应报文，能对 SNMP 报文进行语法分析，ASN.1 和 BER 编码/译码，也能发送陷入报文，并处理 WinSock API 的接口。snmptrap.exe 监听发送给 NT 主机的陷入报文，然后把其中的数据传送给 SNMP 管理 API。

**参考答案**

（49）D

**试题（50）**

Windows Server 2003 中配置 SNMP 服务时，必须以__（50）__身份登录才能完成 SNMP 服务的配置功能。

（50）A. Guest　　B. 普通用户
C. Administrators 组成员　　D. Users 组成员

**试题（50）分析**

本题考查 Windows Server 2003 中有关 SNMP 服务配置的操作权限。

Windows Server 2003 中配置 SNMP 服务时，必须以管理员身份或者 Administrators 组成员身份登录才能完成 SNMP 服务的配置功能。一般用户或者普通用户不能完成 SNMP 配置服务。

**参考答案**

（50）C

**试题（51）**

有一种 NAT 技术叫作“地址伪装”（Masquerading），下面关于地址伪装的描述中正确的是__（51）__。

（51）A. 把多个内部地址翻译成一个外部地址和多个端口号
B. 把多个外部地址翻译成一个内部地址和一个端口号
C. 把一个内部地址翻译成多个外部地址和多个端口号
D. 把一个外部地址翻译成多个内部地址和一个端口号

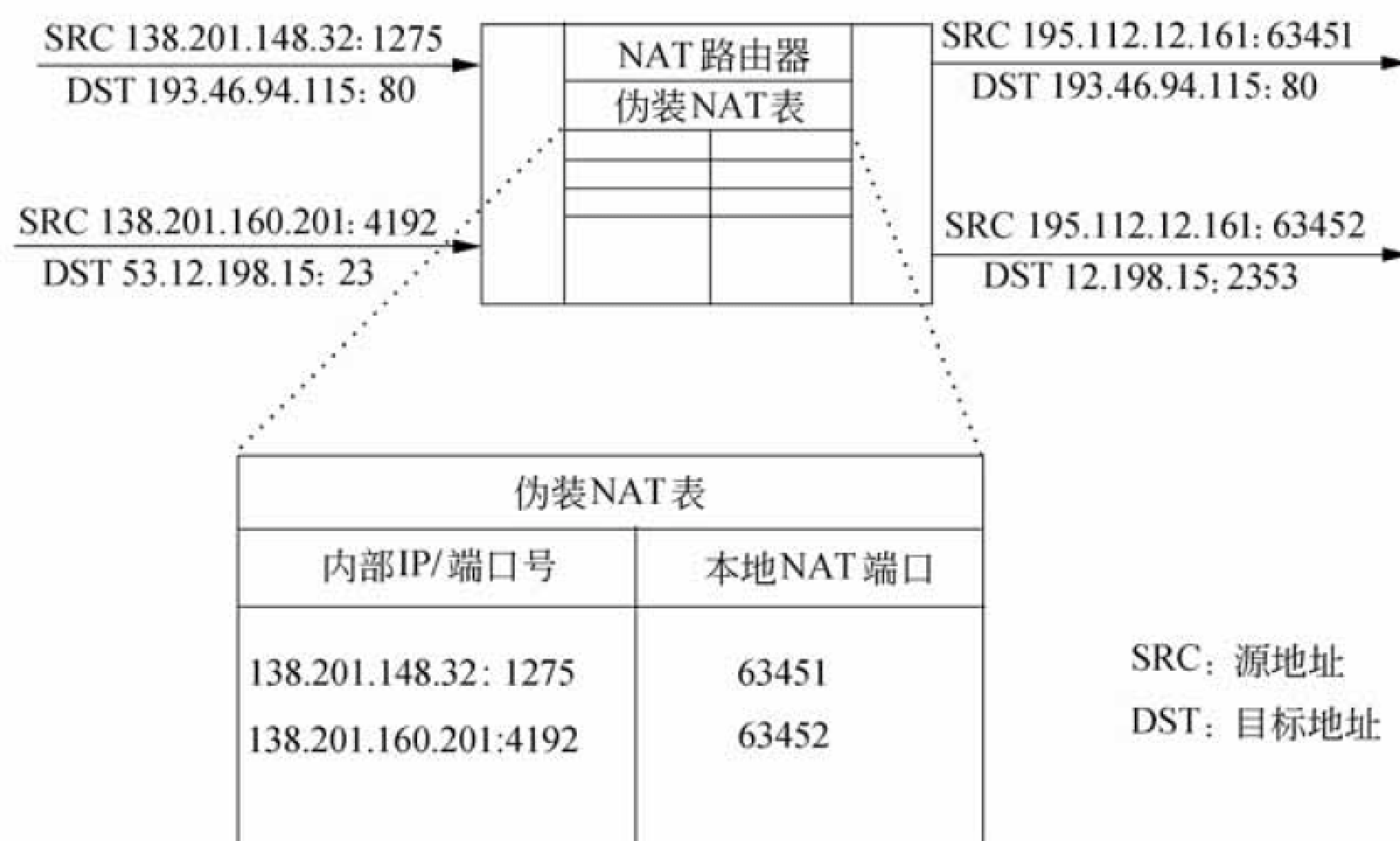
**试题（51）分析**

有一种特殊的 NAT 应用是 m:1 翻译，即把 m 个内部地址翻译成 1 个外部地址和多个端口号。这种技术也叫作伪装（Masquerading），因为用一个路由器的 IP 地址可以把子网中所有主机的 IP 地址都隐蔽起来。如果子网中有多个主机同时都要通信，那么还要对接口号进行翻译，所以这种技术更经常被称为网络地址和端口翻译（Network Address Port Translation，NAPT）。在很多 NAPT 实现中专门保留一部分端口号给伪装使用，叫作伪装端口号。下图中的 NAT 路由器中有一个伪装表，通过这个表对端口号进行翻译，从而隐藏了内部网络 138.201.0.0 中的所有主机。可以看出，这种方法有如下特点：

- 出口分组的源地址被路由器的外部 IP 地址所代替，出口分组的源端口号被一个未使用的伪装端口号所代替；
- 如果进来的分组的目标地址是本地路由器的 IP 地址，而目标端口号是路由器的伪装端口号，则 NAT 路由器就检查该分组是否为当前的一个伪装会话，并试图通过伪装表对 IP 地址和端口号进行翻译。

伪装技术可以作为一种安全手段使用，借以限制外部网络对内部主机的访问。另外

还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。




**参考答案**

（51）A

**试题（52）、（53）**

有一种特殊的 IP 地址叫作自动专用 IP 地址（APIPA），这种地址的用途是＿（52）＿，以下地址中属于自动专用 IP 地址的是＿（53）＿。

（52）A．指定给特殊的专用服务器

B．作为默认网关的访问地址

C．DHCP 服务器的专用地址

D．无法获得动态地址时作为临时的主机地址

（53）A．224.0.0.1　　B．127.0.0.1　　C．169.254.1.15　　D．192.168.0.1

**试题（52）、（53）分析**

自动专用 IP 地址（Automatic Private IP Address，APIPA）是当客户机无法从 DHCP 服务器中获得 IP 地址时自动配置的地址。IANA（Internet Assigned Numbers Authority）为 APIPA 保留了一个 B 类地址块 169.254.0.0～169.254.255.255。当网络中的 DHCP 服务器失效，或者由于网络故障而找不到 DHCP 服务器时，这个功能开始生效，使得客户机可以在一个小型局域网中运行，与其他自动或手工获得 APIPA 地址的计算机进行通信。

**参考答案**

（52）D　（53）C

**试题（54）**

把网络 10.1.0.0/16 进一步划分为子网 10.1.0.0/18，则原网络被划分为＿（54）＿个子网。

（54）A．2　　B．3　　C．4　　D．6

**试题（54）分析**

把子网掩码增加两位，即把原来的网络划分成了 4 个子网。

**参考答案**

（54）C

**试题（55）**

IP 地址 202.117.17.255/22 是什么地址？__（55）__。

（55）A．网络地址　　B．全局广播地址
C．主机地址　　D．定向广播地址

**试题（55）分析**

IP 地址 202.117.17.255/22 的二进制形式是 **11001010.01110101.000100**01.11111111，其中的黑体部分为网络地址，其余的主机地址部分是 01.11111111，可见这是一个主机地址。

**参考答案**

（55）C

**试题（56）**

对下面 4 条路由：202.115.129.0/24、202.115.130.0/24、202.115.132.0/24 和 202.115.133.0/24 进行路由汇聚，能覆盖这 4 条路由的地址是__（56）__。

（56）A．202.115.128.0/21　　B．202.115.128.0/22
C．202.115.130.0/22　　D．202.115.132.0/23

**试题（56）分析**

地址 202.115.129.0/24 的二进制形式为：11001010 01110011 10000001 00000000。

地址 202.115.130.0/24 的二进制形式为：11001010 01110011 10000010 00000000。

地址 202.115.132.0/24 的二进制形式为：11001010 01110011 10000100 00000000。

地址 202.115.133.0/24 的二进制形式为：11001010 01110011 10000101 00000000。

地址 202.115.128.0/21 的二进制形式为：11001010 01110011 10000000 00000000。

所以能覆盖这 4 条路由的地址是 202.115.128.0/21。

**参考答案**

（56）A

**试题（57）、（58）**

可以用于表示地址块 220.17.0.0～220.17.7.0 的网络地址是__（57）__，这个地址块中可以分配__（58）__个主机地址。

（57）A．220.17.0.0/20　　B．220.17.0.0/21
C．220.17.0.0/16　　D．220.17.0.0/24

（58）A．2032　　B．2048　　C．2000　　D．2056

**试题（57）、（58）分析**

8 个地址块的二进制形式是：

220.17.0.0　　11011100.00010001.00000000.00000000

220.17.1.0　　11011100.00010001.00000001.00000000

220.17.2.0　　11011100.00010001.00000010.00000000

220.17.3.0　　11011100.00010001.00000011.00000000

220.17.4.0　　11011100.00010001.00000100.00000000

220.17.5.0　　11011100.00010001.00000101.00000000

220.17.6.0　　11011100.00010001.00000110.00000000

220.17.7.0　　11011100.00010001.00000111.00000000

地址 220.17.0.0　　11011100.00010001.00000000.00000000

可以覆盖这 8 个地址块，每个地址块可以分配 254 个主机地址，共可以分配 254×8=2032 个主机地址。

**参考答案**

（57）B　（58）A

**试题（59）**

下面关于 IPv6 的描述中，最准确的是__（59）__。

（59）A. IPv6 可以允许全局 IP 地址重复使用

B. IPv6 解决了全局 IP 地址不足的问题

C. IPv6 的出现使得卫星联网得以实现

D. IPv6 的设计目标之一是支持光纤通信

**试题（59）分析**

IPv6 解决了全局 IP 地址不足的问题，但是全局 IP 地址不能重复使用。IPv6 可以实现卫星联网，也支持光纤通信，但这些功能在 IPv4 中也是支持的。

**参考答案**

（59）B

**试题（60）**

下面哪个字段的信息出现在 TCP 头部而不出现在 UDP 头部？__（60）__。

（60）A. 目标端口号　　B. 顺序号

C. 源端口号　　D. 校验和

**试题（60）分析**

UDP 是无连接的协议，不需要用顺序号来进行流量和差错控制。UDP 和 TCP 都用端口号来提供向上的多路复用功能，校验和则用于检验协议头出现的差错。

**参考答案**

（60）B

**试题（61）**

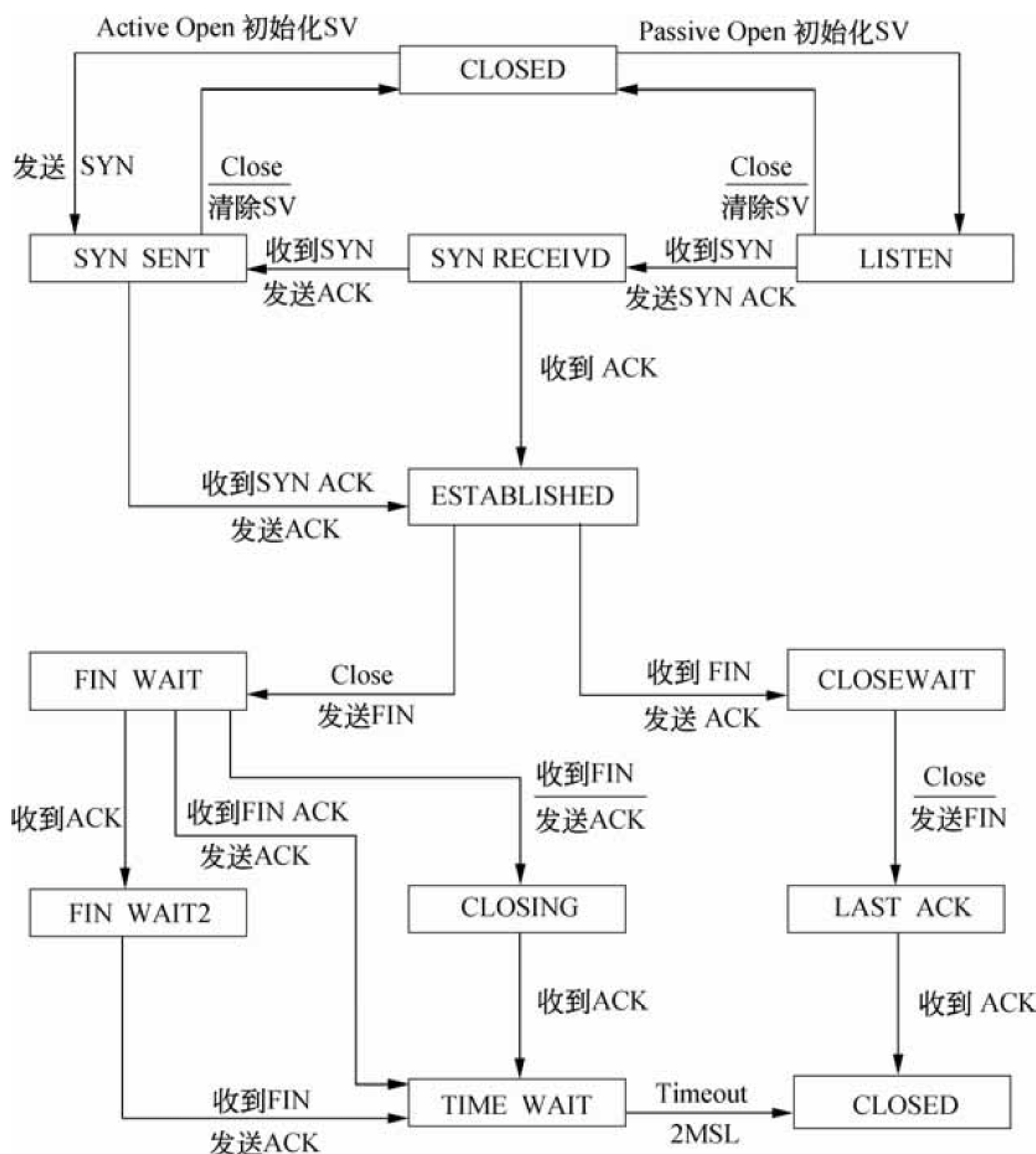
当一个 TCP 连接处于什么状态时等待应用程序关闭端口？（61）。

（61）A. CLOSED　　B. ESTABLISHED

C. CLOSE-WAIT　　D. LAST-ACK

**试题（61）分析**

TCP 建立和释放连接的过程采用三次握手协议。这种协议的实际目的是连接两端都要声明自己的连接端点标识，并回答对方的连接端点标识，以确保不出现错误的连接。连接可能是主动建立的，也可能是被动建立的。在连接建立、存在和释放的各个阶段形成了不同的连接状态，表示在下图中，其中发送和应答的各种信号都是 TCP 段头中的标志。由图可以看出，TCP 连接处于 CLOSE WAIT 状态时等待应用程序关闭端口。




**参考答案**

（61）C

**试题（62）**

一个运行 CSMA/CD 协议的以太网，数据速率为 1Gb/s，网段长 1km，信号速率为 200 000km/sec，则最小帧长是__（62）__比特。

（62）A．1000　　B．2000　　C．10000　　D．200000

**试题（62）分析**

网段长 1km，意味着最远两个结点之间的时延为 $\tau$=5μs，则最小帧长=1Gb/s×2$\tau$=10000 比特。

**参考答案**

（62）C

**试题（63）**

以太网帧结构中“填充”字段的作用是__（63）__。

（63）A．承载任选的路由信息　　B．用于捎带应答

C．发送紧急数据　　D．保持最小帧长

**试题（63）分析**

以太网帧结构中“填充”字段的作用是保持最小帧长，便于检测冲突。如果满足了最小帧长的限制，则在最远的两个站之间出现的发送冲突都会在发送期间检测到。

**参考答案**

（63）D

**试题（64）**

关于无线网络中使用的扩频技术，下面描述中错误的是__（64）__。

（64）A．用不同的频率传播信号扩大了通信的范围

B．扩频通信减少了干扰并有利于通信保密

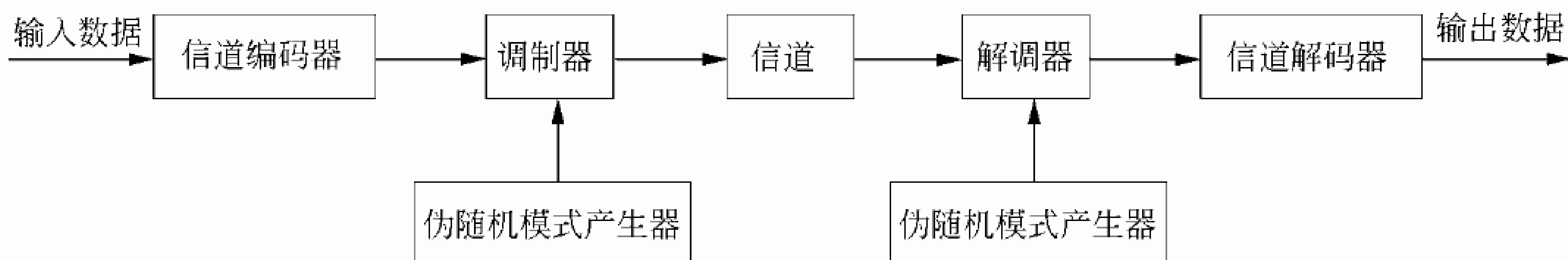
C．每一个信号比特可以用 N 个码片比特来传输

D．信号散布到更宽的频带上降低了信道阻塞的概率

**试题（64）分析**

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（Frequency-Hopping Spread Spectrum，FHSS），更新的版本是直接序列扩展频谱（Direct Sequence Spread Spectrum，DSSS），这两种技术在 IEEE802.11 定义的 WLAN 中都有应用。

下图表示了各种扩展频谱通信系统的共同特点。输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号。再用一个伪随机序列对这个信号进行调制。调制的结果大大拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后再进入信道解码器来恢复数据。




伪随机序列由一个使用初值（称为种子 seed）的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计得好，得到的序列还是能够通过各种随机性测试，这就是被叫作伪随机序列的原因。重要的是除非你知道算法与种子，否则预测序列是不可能的。因此只有与发送器共享一个伪随机序列的接收器才能成功地对信号进行解码。

**参考答案**

（64）A

**试题（65）**

物联网中使用的无线传感网络技术是__（65）__。

（65）A．802.15.1 蓝牙个域网　　B．802.11n 无线局域网

C．802.15.4ZigBee 微微网　　D．802.16m 无线城域网

**试题（65）分析**

IEEE 802.15 工作组负责制定无线个人网（WPAN）的技术规范。这是一种小范围的无线通信系统，覆盖半径仅 10 米左右，可用来代替电脑、手机、PDA、数码相机等智能设备的通信电缆，或者构成无线传感器网络和智能家庭网络等。WPAN 并不是一种与无线局域网（WLAN）竞争的技术，WLAN 可替代有线局域网，而 WPAN 无须基础网络连接的支持，只能提供少量小型设备之间的低速率连接。

IEEE 802.15 工作组划分成四个任务组，分别制定适合不同应用环境的技术标准。802.15.1 采用了蓝牙技术规范，这是最早实现的面向低速率应用的 WPAN 标准，主要开发工作由蓝牙专业组（SIG）来做，其研究成果由 IEEE LAN/MAN 标准委员会颁布为正式标准。

802.15.2 对蓝牙网络与 802.11b 网络之间的共存提出了建议。这两种网络都采用了免许可证的 2.4GHz 频段，它们之间会产生通信干扰，要在共享环境中协同工作，必须采用 802.15.2 提出的交替无线介质访问（AWMA）和分组通信仲裁（PTA）方案。

802.15.3 把目标瞄准了低复杂性、低价格、低功耗的消费类电子设备，为其提供至少 20Mb/s 的高速无线连接。2003 年 8 月批准的 IEEE 802.15.3 采用 64-QAM 调制，数据速率高达 55 Mb/s，适合于短时间内传送大量的多媒体文件。在人手可及的范围内，多个电子设备可以组成一个无线 Ad Hoc 网络，802.15 把这种网络叫作 piconet，通常翻译为微微网。802.15.3 给出的 piconet 网络模型的特点是，各个电子设备（DEV）可以独立地互相通信，其中一个设备可以作为通信控制的协调器 PNC，负责网络定时和向 DEV

发放令牌，获得令牌的 DEV 才可以发送通信请求。PNC 还具有管理 QoS 需求和调节电源功耗的功能。IEEE 802.15.3 定义了微微网的介质访问控制协议和物理层技术规范，适合于多媒体文件传输的需求。

与 802.15.3 相反，802.15.4 则瞄准了速率更低距离更近的无线个人网。802.15.4 标准适合于固定的、手持的或移动的电子设备，这些设备的特点是使用电池供电，电池寿命可以长达几年时间，通信速率可以低至 9.6Kb/s，从而实现低成本的无线通信。802.15.4 标准的研发工作主要由 ZigBee 联盟来做。所谓 ZigBee 是指蜜蜂跳的“之”字形舞蹈，蜜蜂用跳舞来传递信息，告诉同伴蜜源的位置。“ZigBee”形象地表达了通过网络结点之间互相传递，将信息从一个结点传输到远处另外一个结点的通信方式。

**参考答案**

（65）C

**试题（66）**

正在发展的第四代无线通信技术推出了多个标准，下面的选项中不属于 4G 标准的是（66）。

（66）A．LTE　B．WiMAXII　C．WCDMA　D．UMB

**试题（66）分析**

候选的 4G 标准有 3 个：分别是 UMB （ultra mobile broadband）、LTE （long-term evolution）和 WiMAX II （IEEE 802.16m）。

超级移动宽带 UMB 是由高通公司为首的 3GPP2 组织推出的 CDMA-2000 的升级版。UMB 的最高下载速率可达到 288Mb/s，最高上传速率可达到 75Mb/s，支持的终端移动速率超过 300km/h。

长期演进 LTE（Long Term Evolution）是沿着 GSM—W-CDMA—4G 路线发展的技术，是由以欧洲电信为首的 3GPP 组织启动的新技术研发项目。同 UMB 一样，LTE 也采用了 OFDM/OFDMA 作为物理层的核心技术。

2006 年 12 月批准的 802.16m 是向 IMT-Advanced 迈进的研究项目。为了达到 4G 的技术要求，IEEE802.16m 的下行峰值速率在低速移动、热点覆盖条件下可以达到 1Gb/s，在高速移动、广域覆盖条件下可以达到 100Mb/s。为了向前兼容，802.16m 准备对 802.16e 采用的 OFDMA 调制方式进行增补，进一步提高系统吞吐量和传输速率。

UMB、LTE 和移动 WiMAX 虽然各有差别，但是它们的共同之处是都采用 OFDM 和 MIMO 技术来提供更高的频谱利用率。在未来的发展过程中，哪一种技术将会胜出，哪一种技术将会被淘汰，尚很难预料。

**参考答案**

（66）C

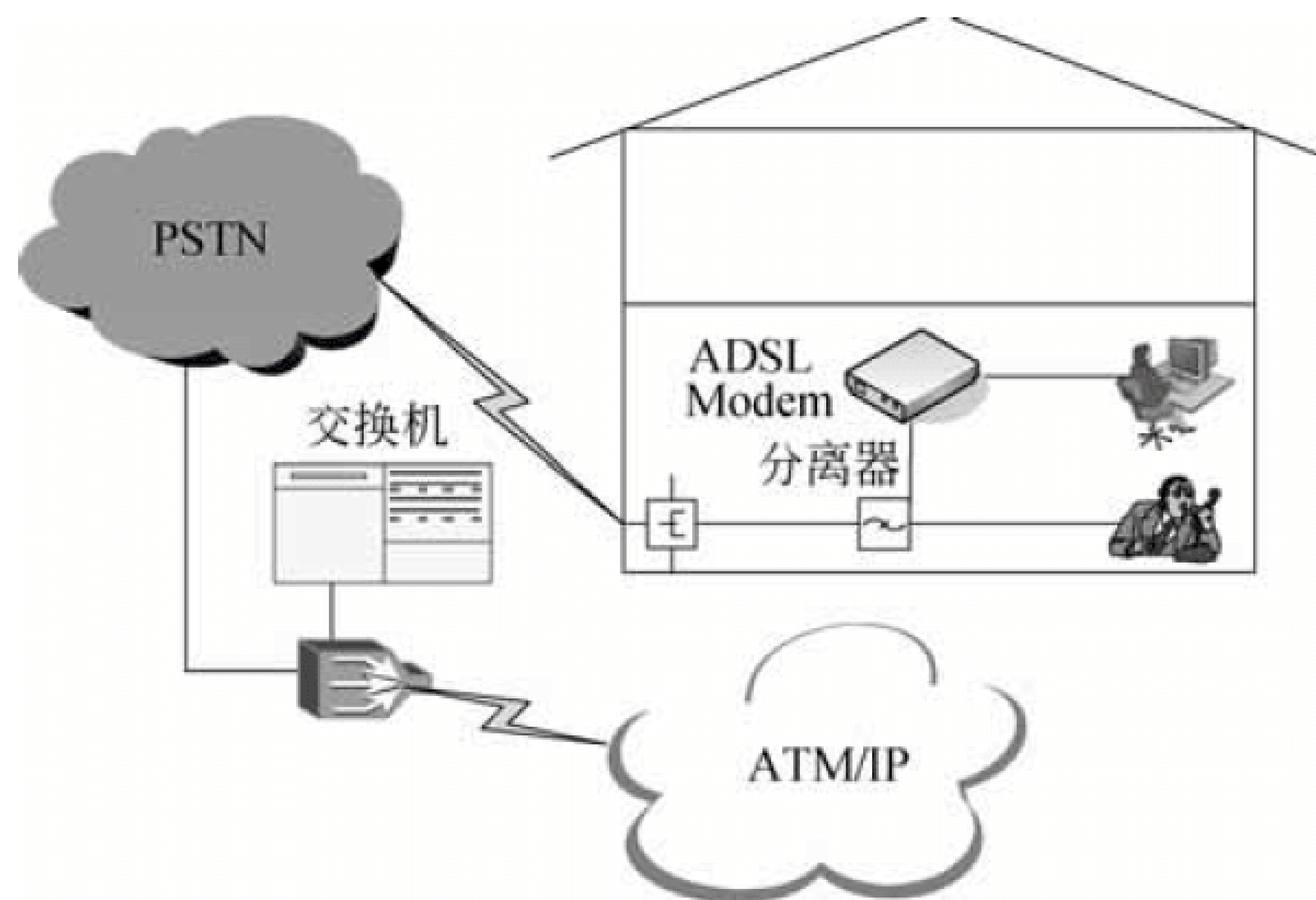
**试题（67）、（68）**

下面是家庭用户安装 ADSL 宽带网络时的拓扑结构图，图中左下角的 X 是（67）设

备，为了建立虚拟拨号线路，在用户终端上应安装__（68）__协议。

（67）A．DSLAM　B．HUB　C．ADSL Modem　D．IP Router

（68）A．ARP　B．HTTP　C．PPTP　D．PPPoE




**试题（67）、（68）分析**

ADSL 是一种非对称 DSL 技术，在一对铜线上可提供上行速率 512Kb/s～1Mb/s，下行速率 1～8Mb/s，有效传输距离在 3～5km 左右。ADSL 在进行数据传输的同时还可以使用第三个信道提供 4kHz 的语音传输。现在比较成熟的 ADSL 标准有两种，即 G.DMT 和 G.Lite。G.DMT 是全速率的 ADSL 标准，支持 8Mb/s 的下行速率及 1.5Mb/s 的上行速率，但 G.DMT 要求用户端安装 POTS 分离器，技术复杂而且价格昂贵。G.Lite 标准速率较低，下行速率为 1.5Mb/s，上行速率为 512Kb/s，但省去了 POTS 分离器，成本较低且便于安装。G.DMT 较适用于小型办公室（SOHO）应用，而 G.Lite 则更适用于普通家庭应用。

ADSL 需要的接入设备包括局端接入设备 DSLAM 和用户端设备 ATU-R，以及用户线路和管理服务器。DSLAM 作为 ADSL 的局端收发设备由运营商提供，实现用户接入和集中复用功能，同时提供不对称的流量控制机制。用户端设备 ATU-R 就是 ADSL Modem，可以实现 POTS 语音与数据的分离，完成用户端 ADSL 数据的接收和发送。ADSL 采用双绞线作为传输介质，无需对现有的用户线路进行改造就可直接使用。管理服务器主要是宽带接入服务器（BRAS），能够提供 ADSL 用户接入的终结、认证、计费、管理等基本业务，此外还可以提供防火墙、安全控制、NAT 转换、带宽管理、流量控制等网络业务管理功能。ADSL 采用的调制技术有 3 种：

- QAM（Quadrature Amplitude Modulation）
- CAP（Carrierless Amplitude-Phase modulation）
- DMT（Discrete Multitone）

离散多音（DMT）调制技术的传输质量较佳，被广泛采用。DMT 在铜质电话线上

将从直流到 1MHz 的频带划分成 256 个子信道，每个子信道带宽 4.3kHz。频率最低的信道（0～4.3KHz）用来传输模拟电话信号，其余频带在低频部分传输上行信号，高频部分传输下行信号。ADSL Modem 独立地分析每个信道的信噪比，以确定该信道可适用的数据速率。当某一信道的信噪比恶化时，Modem 自动降低该信道的数据速率，以保证传输的正确性。如果一个信道的信噪比极其恶化，甚至可能将其关闭。上、下行信号的分割有两种办法：频率分割法（FDM）和回波抵消法（EC），现在市场上的 ADSL 产品绝大多数采用频分法。

ADSL 接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装 PPPoE（PPP over Ethernet）或PPPoA（PPP over ATM）客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址，开机即可接入 Internet。

**参考答案**

（67）A　（68）D

**试题（69）**

网络系统设计过程中，物理网络设计阶段的任务是__（69）__。

（69）A．依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B．分析现有网络和新网络的各类资源分布，掌握网络的状态

C．根据需求规范和通信规范，实施资源分配和安全规划

D．理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

**试题（69）分析**

物理网络是逻辑网络的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。

**参考答案**

（69）A

**试题（70）**

下列关于网络核心层的描述中，正确的是__（70）__。

（70）A．为了保障安全性，应该对分组进行尽可能多的处理

B．将数据分组从一个区域高速地转发到另一个区域

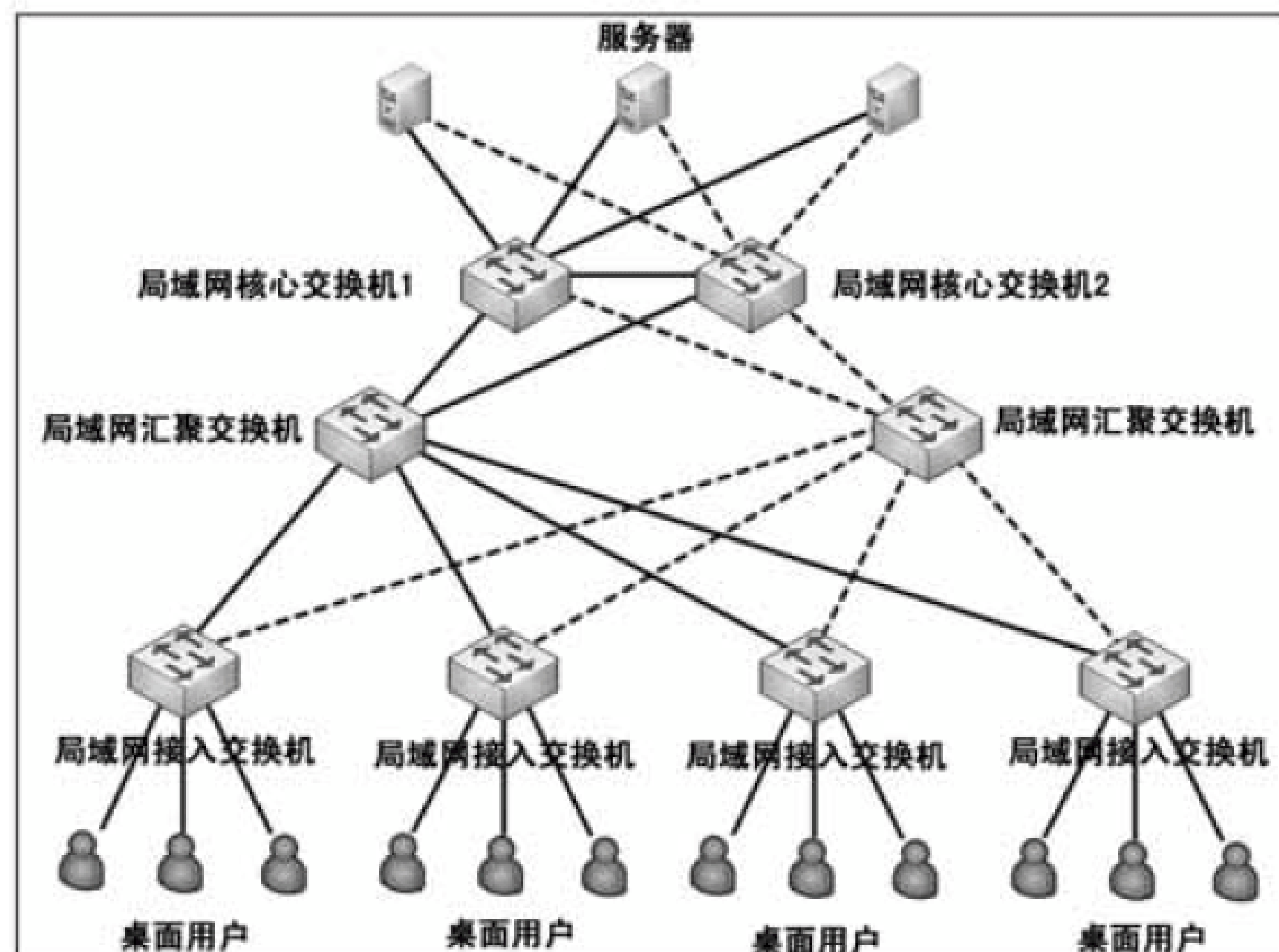
C．由多台二、三层交换机组成

D．提供多条路径来缓解通信瓶颈

**试题（70）分析**

局域网的层次结构是将局域网络划分成不同的功能层次，例如划分成核心层、汇聚层和接入层，通过与核心设备互连的路由器接入广域网。典型的层次结构如下图所示。层次结构的特点如下：

- 网络功能划分清晰，有利发挥联网设备的最大效率；
- 网络拓扑结构使得故障定位可分级进行，便于维护；
- 便于网络拓扑的后续扩展。




在三层模型中，核心层提供不同区域之间的高速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。

在设计核心层设备的功能时应避免使用数据包过滤、策略路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的可管理性。

核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。

核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。

汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。

如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问；

接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等；

接入层要负责收集用户信息（例如用户 IP 地址、MAC 地址、访问日志等），作为计费和排错的依据。

**参考答案**

（70）B

**试题（71）～（75）**

Let us now see how randomization is done when a collision occurs. After a （71）, time is divided into discrete slots whose length is equal to the worst-case round-trip propagation time on the ether(2τ). To accommodate the longest path allowed by Ethernet, the slot time has been set to 512 bit times, or 51.2μsec.

After the first collision, each station waits either 0 or 1 （72） times before trying again. If two stations collide and each one picks the same random number, they will collide again. After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times. If a third collision occurs (the probability of this happening is 0.25), then the next time the number of slots to wait is chosen at （73） from the interval 0 to $2^3$-1.

In general, after *i* collisions, a random number between 0 and $2^i$-1 is chosen, and that number of slots is skippeD. However, after ten collisions have been reached, the randomization （74） is frozen at a maximum of 1023 slots. After 16 collisions, the controller throws in the towel and reports failure back to the computer. Further recovery is up to （75） layers.

（71）A. datagram　B. collision　C. connection　D. service

（72）A. slot　B. switch　C. process　D. fire

（73）A. rest　B. random　C. once　D. odds

（74）A. unicast　B. multicast　C. broadcast　D. interval

（75）A. local　B. next　C. higher　D. lower

**参考译文**

现在让我们看看当冲突发生时，随机性操作是如何体现的。出现冲突时，时间被划分为离散的时槽，其长度等于最坏情况下以太网的周转传播时间（2τ），为了适应以太网中的最长通路，时槽被设为 512 比特的发送时间，即 51.2 微妙。

第一次冲突后，每个站在再次试图发送前等待 0 或 1 个时槽。如果两个站出现了冲突，并且每个站都选用了同样的随机数，那么就会再一次发生冲突。第二次发生冲突后，每个站随机地选取数字 0、1、2 或者 3，并等待相应的时槽数。如果发生了第三次冲突（这种情况出现的概率为 0.25），则下一次等待的时槽数目就随机地在 0~$2^3$-1 中选取。

一般情况下，第 *i* 次冲突后，随机数在 0 到 $2^i$-1 之间选取，相应的时槽数被跳过。然而，达到 10 次冲突后，随机数被固定在最大 1023 个时槽之内。16 次冲突后，控制器放弃发送，向计算机发出故障报告。进一步的恢复措施由上层协议实施。

**参考答案**

（71）B　（72）A　（73）B　（74）D　（75）C

# 第 16 章　2012 下半年网络工程师下午试题分析与解答

试题一（共 20 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某学校有三个校区，校区之间最远距离达到 61km，学校现在需要建设校园网，具体要求如下：校园网通过多运营商接入互联网，主干网采用千兆以太网将三个校区的中心节点连起来，每个中心节点都有财务、人事和教务三类应用。按应用将全网划分为 3 个 VLAN，三个中心都必须支持 3 个 VLAN 的数据转发。路由器用光纤连到校区 1 的中心节点上，距离不超过 500 米，网络结构如图 1-1 所示。

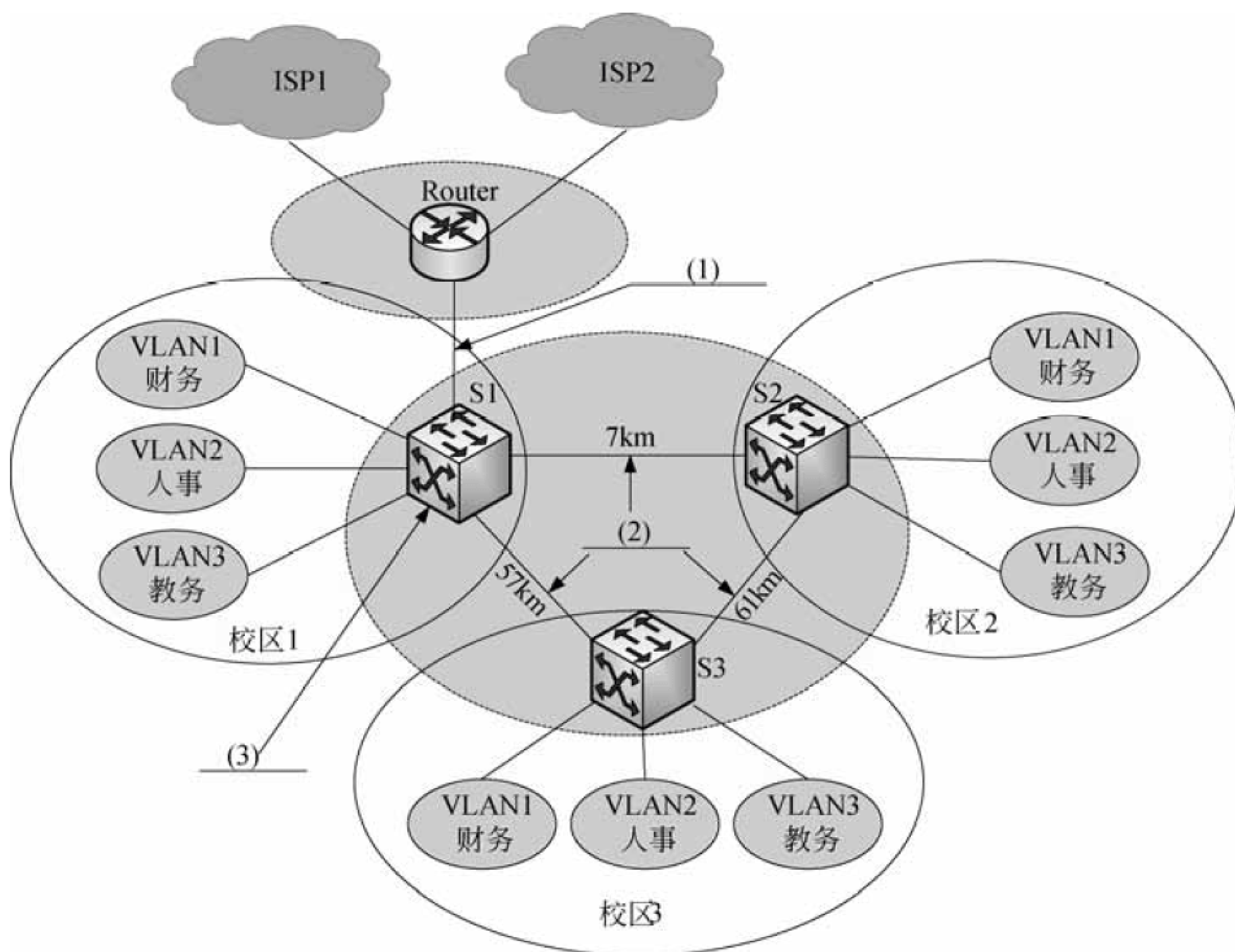



图 1-1

【问题 1】（3 分）

根据题意和图 1-1，从经济性和实用性出发填写网络拓扑图中所用的传输介质和设备。

（1）～（3）备选答案：

A．3 类 UTP　　B．5 类 UTP　　C．6 类 UTP
D．单模光纤　　E．多模光纤　　F．千兆以太网交换机
G．百兆以太网交换机　　H．万兆以太网交换机

**【问题 2】（4 分）**

如果校园网中办公室用户没有移动办公的需求，采用基于__（4）__的 VLAN 划分方法比较合理；如果有的用户需要移动办公，采用基于__（5）__的 VLAN 划分方法比较合适。

**【问题 3】（6 分）**

图 1-1 中所示的交换机和路由器之间互连的端口类型全部为标准的 GBIC 端口，表 1-1 列出了互联所用的光模块的参数指标，请根据组网需求从表 1-1 中选择合适的光模块类型满足合理的建网成本，Router 和 S1 之间用__（6）__互联，S1 和 S2 之间用__（7）__互联，S1 和 S3 之间__（8）__用互联，S2 和 S3 之间用__（9）__互联。

**表 1-1**

| 光模块类型 | 支持的参数指标 | | | |
|---|---|---|---|---|
| | 标　　准 | 波　长 | 光纤类型 | 备　　注 |
| 模块 1 | 1000BaseSX | 850nm | 62.5/125μm<br>50/125μm | 多模，价格便宜 |
| 模块 2 | 1000BaseLX/1000BaseLH | 1310nm | 62.5/125μm<br>50/125μm<br>9/125μm | 单模，价格稍高 |
| 模块 3 | 1000BaseZX | 1550nm | 9/125μm | 单模，价格昂贵 |

**【问题 4】（3 分）**

如果将 Router 和 S1 之间互连的模块与 S1 和 S2 之间的模块互换，Router 和 S1 以及 S1 和 S2 之间的网络是否能联通？并请解释原因。

**【问题 5】（4 分）**

若 VLAN3 的网络用户因为业务需要只允许从 ISP1 出口访问 Internet，在路由器上需进行基于__（10）__的策略路由配置。其他 VLAN 用户访问 Internet 资源时，若访问的是 ISP1 上的网络资源，则从 ISP1 出口；若访问的是其他网络资源，则从 ISP2 出口，那么在路由器上需进行基于__（11）__的策略路由配置。

**试题一分析**

本题考查网络规划、网络设备模块选型以及网络配置方面的知识。

**【问题 1】**

本问题考查网络传输介质以及网络设备的选用知识。根据网络的需求和拓扑图，传输介质 1 连接出口路由器和网络中心节点交换机，两台设备之间距离不超过 500 米，且

网络要求用光纤连接，又因为题目要求经济性，所以应该采用多模光纤。传输介质 2 连接三个校区的中心交换机，三个中心之间距离最小 7km，所以应该采用单模光纤。网络设备 3 连接出口路由器和其他两个校区的节点交换机，网络要求主干网采用千兆以太网，本着经济性并满足要求的目的，应该采用千兆以太网交换机。

**【问题 2】**

本问题考查交换机 VLAN 划分知识。

VLAN 的划分方法有基于端口划分、基于 MAC 地址划分等。

基于端口的 VLAN，简单的讲就是交换机的一个端口就是一个虚拟局域网，凡是连接在这个端口上的主机属于同个虚拟局域网之中。基于端口的 VLAN 的优点为：由于一个端口就是一个独立的局域网。所以，当数据在网络中传输的时候，交换机就不会把数据包转发给其他的端口，如果用户需要将数据发送到其他的虚拟局域网中，就需要先由交换机发往路由器再由路由器发往其他端口；同时以端口为中心的 VLAN 中完全由用户自由支配端口，无形之中就更利于管理。但是以端口为中心的 VLAN，当用户位置改变时，往往也伴随着用户位置的改变而对网线也要进行迁移。如果不会经常移动客户机的话，可以采用这种方式。从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

基于 MAC 地址划分 VLAN 的方法。这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN，这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。

根据需求描述，没有移动办公需求的可考虑采用基于端口的 VLAN 划分方法；有移动办公需求的可考虑采用基于 MAC 的 VLAN 划分方法。

**【问题 3】**

本问题考查网络设备配置的光模块的相关知识。

根据网络拓扑和题目需求描述可知，考虑建网成本和实际联网网络介质可知选择满足需求的光纤模块即可。Router 和 S1 之间传输介质为多模光纤，因此采用多模光模块。S1 和 S2 之间距离 7km，采用波长为 1310nm 的可传输 10km 的单模光模块即可。S1 和 S3 以及 S2 和 S3 之间距离大于 50KM，只能采用波长为 1550nm 的远距离传输的单模光模块。

**【问题 4】**

本问题考查实际组网工程中光模块的使用知识。

因为波长为 1310nm 的光波可以在 62.5/125μm、50/125μm 以及 9/125μm 的传输介质中传输，也就是说可以在多模光纤中传输，因此 Router 与 S1 之间仍然可以通信；但是波长为 850nm 的光波不能在 9/125μm 的单模光纤中传输，因此 S1 与 S2 之间不能通信。

【问题 5】

本问题考查路由器有关策略路由的相关配置知识。

传统的路由只能根据目的地址进行报文转发，策略路由相对来说就比较灵活了，可以根据源地址、目的地址、协议类型、报文大小等进行路由转发。在进行路由转发的时候，路由器根据已经设定的策略对数据包进行匹配，如果匹配到一条策略，就用该策略进行转发，如果没有匹配到，就根据路由表中的路由进行转发。策略路由主要应用在路由表复杂或者需要对路由进行控制的情况下，特别是当网络出口有两条及以上，需要对不同服务和应用或者不同客户端的路由进行控制时。对于网络用户访问网络资源时的不同需求，如一部分用户仅需访问某个 ISP，可考虑根据源地址进行路由转发；另一部分用户的网络访问根据目的 IP 有所不同时可考虑采用基于目的地址的策略路由。

**参考答案**

【问题 1】

（1）E

（2）D

（3）F

【问题 2】

（4）交换机端口

（5）MAC 地址

【问题 3】

（6）模块 1

（7）模块 2

（8）模块 3

（9）模块 3

【问题 4】

Router 与 S1 通，S1 与 S2 不通，因为模块 2 的传输介质兼容多模光纤，模块 1 的传输介质不兼容单模光纤。

【问题 5】

（10）源地址

（11）目的地址

**试题二（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司搭建了一个小型局域网，网络中配置一台 Linux 服务器作为公司内部文件服务器和 Internet 接入服务器，该网络结构如图 2-1 所示。

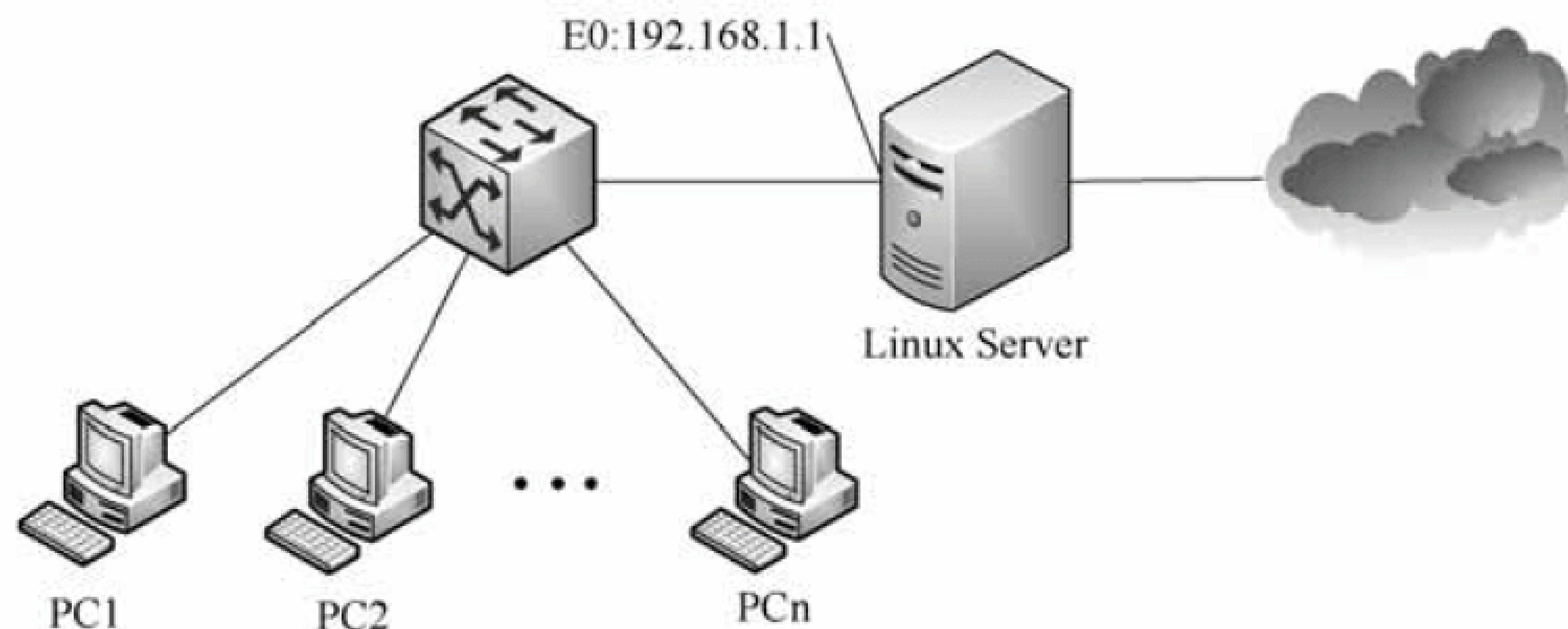



图 2-1

**【问题 1】（5 分）**

Linux 的文件传输服务是通过 vsftpd 提供的，该服务使用的应用层协议是__（1）__协议，传输层协议是__（2）__协议，默认的传输层端口号为__（3）__。

vsftpd 服务可以通过命令行启动或停止，启动该服务的命令是__（4）__，停止该服务的命令是__（5）__。

**【问题 2】（5 分）**

vsftpd 程序主配置文件的文件名是__（6）__。若当前配置内容如下所示，请给出对应配置项和配置值的含义。

```
…
listen_address=192.168.1.1
#listen_port=21
#max_per_ip=10
#max_clients=1000
anonymous_enable=YES          （7）
local_enable=YES              （8）
write_enable=YES              （9）
userlist_enable=YES           （10）
…
```

**【问题 3】（2 分）**

为了使因特网上的用户也可以访问 vsftpd 提供的文件传输服务，可以通过简单的修改上述主配置文件实现，修改的方法是__（11）__。

**【问题 4】（3 分）**

由于 Linux 服务器的配置较低，希望限制同时使用 FTP 服务的并发用户数为 10，每个用户使用 FTP 服务时可以建立的连接数为 5，可以通过简单的修改上述主配置文件实现，修改的方法是__（12）__。

**试题二分析**

本题主要考查考生对 Linux 系统中 FTP 服务 vsftpd 配置等相关知识及应用。

**【问题 1】**

Linux 的文件传输服务是通过 vsftpd 提供的，该服务使用的应用层协议是文件传输协议（FTP），文件传输协议 FTP 采用的传输层协议是有连接的、可靠的 TCP 协议，FTP 协议默认的传输层端口号为 21，FTP 服务默认值该端口上提供服务。

Linux 中的所有服务都可以通过 service 命令从命令行启动或停止，命令的格式是：service 服务程序名称 start/stop。

vsftpd 服务可以通过命令行启动或停止，启动该服务的命令是 service vsftpd start，停止该服务的命令是 service vsftpd stop。

**【问题 2】**

vsftpd 程序主配置文件的文件名是 vsftpd.conf，该文件缺省安装于/etc/vsftpd 目录中。该配置文件中所有参数的配置形式均为“参数=值”的方式，关键字对大小写敏感，以“#”开始的是注释行，注释行在执行时被忽略。

vsftpd.conf 配置文件中的配置项非常多，下面仅对题目中出现的配置项做出解释，其余配置项和相关含义请参看联机手册。

listen_address=192.168.1.1
指定服务监听的 IP 地址，如果没有该配置项则默认//监听本机的所有 IP 地址

listen_port=21
指定服务监听的端口号，默认值是 21

max_per_ip=10
指定每一给定 IP 地址的客户端的最大连接数

max_clients=1000
指定服务器可以同时提供服务的客户端数量

anonymous_enable=YES
允许匿名用户登录

local_enable=YES
允许 Linux 系统中的本地用户登录

write_enable=YES
允许用户上传文件

userlist_enable=YES
userlist 文件有效，此时默认禁止 userlist 文件中的用户登录，如果要允许 userlist 文件中的用户登录，需要增加另一配置项 userlist_deny=NO。

**【问题 3】**

因为配置文件 vsftpd.conf 中有配置项 listen_address=192.168.1.1，即 FTP 服务仅仅在内网所在地址上监听，因特网上的用户无法访问，为了使因特网上的用户也可以访问 vsftpd 提供的文件传输服务，只需注释该配置项即可。

**【问题4】**

由于Linux服务器的配置较低，希望限制同时使用FTP服务的并发用户数为10，每个用户使用FTP服务时可以建立的连接数为5，可以通过简单的修改上述主配置文件实现，修改的方法是设置max_per_ip=5，max_clients=10。

**参考答案**

**【问题1】**

（1）FTP

（2）TCP

（3）21

（4）service vsftpd start

（5）service vsftpd stop

**【问题2】**

（6）vsftpd.conf

（7）允许匿名用户访问

（8）允许本地用户访问

（9）允许用户上传文件

（10）禁止用户列表文件中的用户访问

**【问题3】**

(11) 注释或删除“listen_address=192.168.1.1”配置项

**【问题4】**

（12）改“#max_per_ip=10”为“max_per_ip=5”，改“#max_clients=1000”为“max_clients=10”

**试题三（共20分）**

阅读以下说明，回答问题1至问题7，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位网络拓扑结构如图3-1，该单位Router以太网接口E0接内部交换机S1，S0接口连接到电信ISP的路由器；交换机S1连接内部的Web服务器、DHCP服务器、DNS服务器和部分客户机，服务器均安装Windows Server 2003，办公室的代理服务器（Windows XP系统）安装了两块网卡，分别连接交换机S1、S2，交换机S1、S2的端口均在VLAN1中。

**【问题1】（4分）**

根据图3-1，该单位Router S0接口的IP地址应设置为__（1）__；在S0接口与电信ISP路由器接口构成的子网中，广播地址为__（2）__。

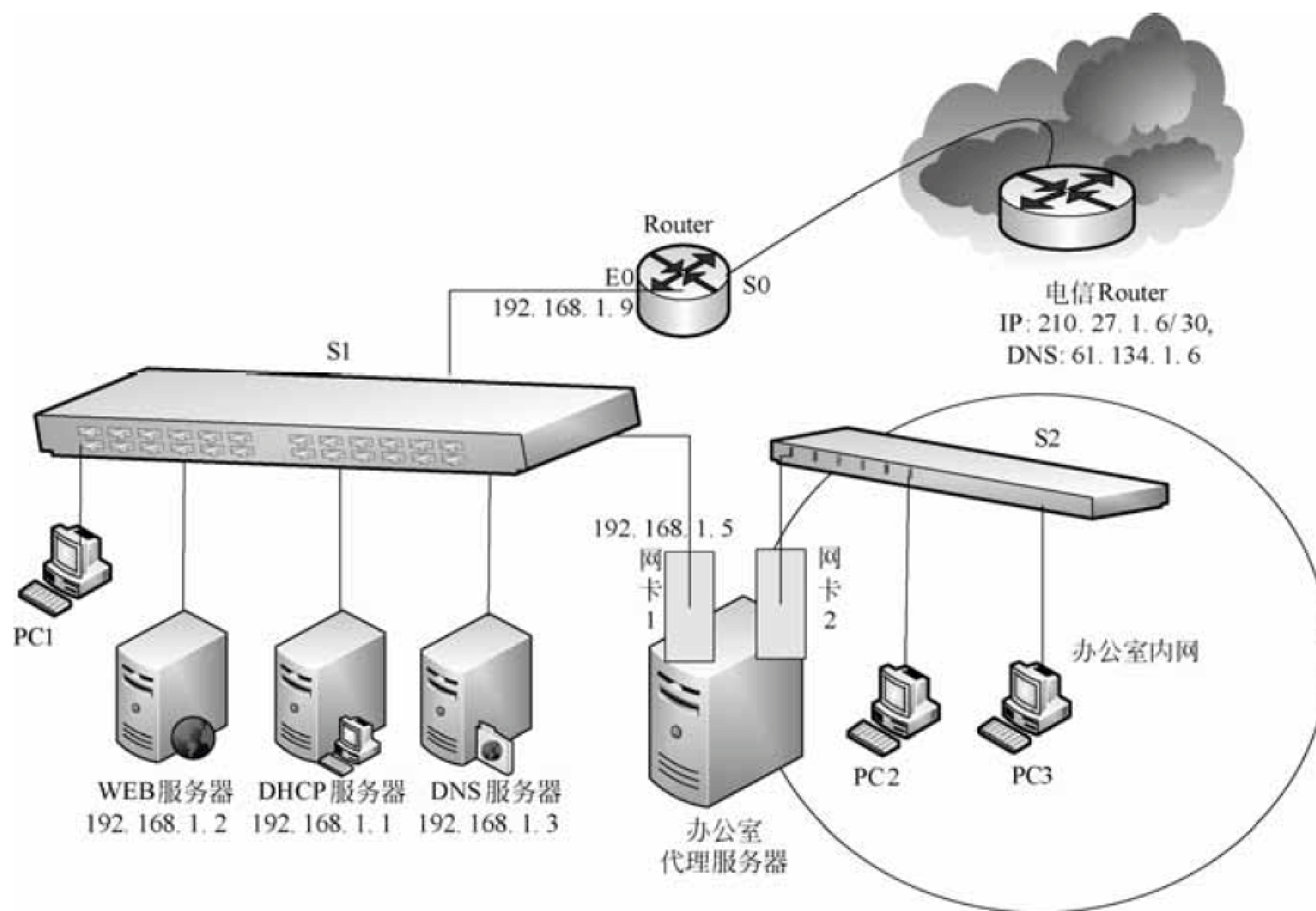



图 3-1

**【问题 2】（2 分）**

办公室代理服务器的网卡 1 为静态地址，在网卡 1 上启用 Windows XP 内置的“Internet 连接共享”功能，实现办公室内网的共享代理服务；那么通过该共享功能自动分配给网卡 2 的 IP 地址是__（3）__。

**【问题 3】（2 分）**

在 DHCP 服务的安装过程中，租约期限一般默认为__（4）__天。

**【问题 4】（2 分）**

该单位路由器 Router 的 E0 口设置为 192.168.1.9/24，若在 DHCP 服务器上配置、启动、激活 DHCP 服务后，查看 DHCP 地址池的结果如图 3-2 所示。

为了满足图 3-1 的功能，在 DHCP 服务器地址池配置操作中还应该增加什么操作？

**【问题 5】（3 分，每空 1 分）**

假如在图 3-1 中移除 DHCP 服务器，改由单位 Router 来提供 DHCP 服务，在 Router 上配置 DHCP 服务时用到了如下命令，请在下划线处将命令行补充完整。

```
Router(config)# ip__(5)__ hkhk    //配置 DHCP 地址池名为 hkhk
Router(dhcp-config)#__(6)__ 192.168.1.0  255.255.255.0
Router(dhcp-config)#__(7)__192.168.1.9
```

**【问题 6】（4 分，每空 2 分）**

在网站的属性窗口中，若“QQQ 属性”选项卡的“IP 地址”选项设置为“全部未

分配”，如图 3-3 所示，则说明___（8）___。

（8）备选答案：

A. 网站的 IP 地址为 192.168.1.1，可以正常访问

B. 网站的 IP 地址为 192.168.1.2，可以正常访问

C. 网站的 IP 地址未分配，无法正常访问




图 3-2




图 3-3

在图 3-4 的 Web 服务主目录选项卡上，至少要设置对主目录的（9）权限，才能访问该 Web 服务器。

（9）备选答案：

A. 读取　　B. 写入　　C. 目录浏览　　D. 记录访问

**【问题 7】(3 分)**

按系统默认的方式配置了 KZ 和 QQQ 两个网站（如图 3-5 所示），此时两个网站均处于停止状态，若要使这两个网站能同时工作，请给出三种可行的解决办法。

方法一：___（10）___；

方法二：___（11）___；

方法三：___（12）___。

**试题三分析**

本题考查 IP 地址配置、网络代理、以及 Windows Server 2003 有关网络组件配置的应用。

**【问题 1】**

考查 IP 地址根据子网掩码的配置分配，根据 ip 信息 210.27.1.6/30，可知：该子网的子网掩码是 255.255.255.252，该子网是 210.27.1.4，广播地址为 210.27.1.7，因为 210.27.1.6 已用，故 Router S0 接口的 IP 地址只能设置为 210.27.1.5。

所以（1）的正确答案 210.27.1.5，（2）的正确答案 210.27.1.7。




图 3-4




图 3-5

【问题 2】

根据图上的设计，通过网卡 2 实现办公室内网的共享代理服务，在 Windows XP 内置的“Internet 连接共享”功能中，自动分配给代理网卡网卡 2 的 IP 地址是 192.168.0.1。

【问题 3】

在 Windows 2003 Server 的网络组件 DHCP 服务的安装过程中，按照操作系统的设置，租约期限一般默认为 8 天。

【问题 4】

本问题考查 DHCP 服务器的配置，结合图 3-1 和图 3-2，可看到图 3-2 中 DHCP 的 IP 地址池范围设置了 192.168.1.1 到 254，但是在该子网中，已经把 192.168.1.1、192.168.1.2、192.168.1.3、192.168.1.5、192.168.1.9 静态分配给了其他设备，所以还要进行“添加排除 IP 地址的操作”，要把上述 5 个已用了的 IP 排除掉。

【问题 5】

本问题考查对路由器 DHCP 功能的配置操作，CISCO 路由器的配置命令序列如下：

```
Router(config)# ip  dhcp pool   hkhk
Router(dhcp-config)#  network  192.168.1.0  255.255.255.0
Router(dhcp-config)#  default-router   192.168.1.9
```

【问题 6】

本问题空（8）考查对 WEB 网站服务器配置的操作，如图 3-3 所示，“IP 地址”选项中的“(全部未分配)”的意思是对配置过 Web 服务的任何地址都可以 Web 访问，结合图 3-1，知道 Web 服务器的 IP 是 192.168.1.2，所以该题（8）的答案是“网站的 IP 地址为 192.168.1.2，可以正常访问”。

本问题（9）考查对 Web 服务器配置中权限有关的设置，要设置对 Web 主目录的“读取”权限，才能正常访问该 Web 服务器。

【问题 7】

本问题考查对 Web 网站服务器配置操作时，当在一台服务器上配置多个 Web 服务时，应该怎么避免冲突。常用的方法是：

方法一：给 KZ 和 QQQ 两个服务器指定不同的 IP 地址；

方法二：给 KZ 和 QQQ 两个服务器指定不同的主机头值；

方法三：给 KZ 和 QQQ 两个服务器指定不同的端口号。

**参考答案**

【问题 1】

（1）210.27.1.5

（2）210.27.1.7

【问题 2】

（3）192.168.0.1

【问题 3】

（4）8 天

【问题 4】

进行“添加排除”IP 地址的操作

【问题 5】

（5）dhcp pool

（6）network

（7）default-router

【问题 6】

（8）B

（9）A

【问题 7】

（10）给 KZ 和 QQQ 指定不同的 IP 地址

（11）给 KZ 和 QQQ 指定不同的主机头值

（12）给 KZ 和 QQQ 指定不同的端口号

（10）～（12）位置可互换

**试题四（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某单位网络结构如图 4-1 所示，其中维护部通过 DDN 专线远程与总部互通。

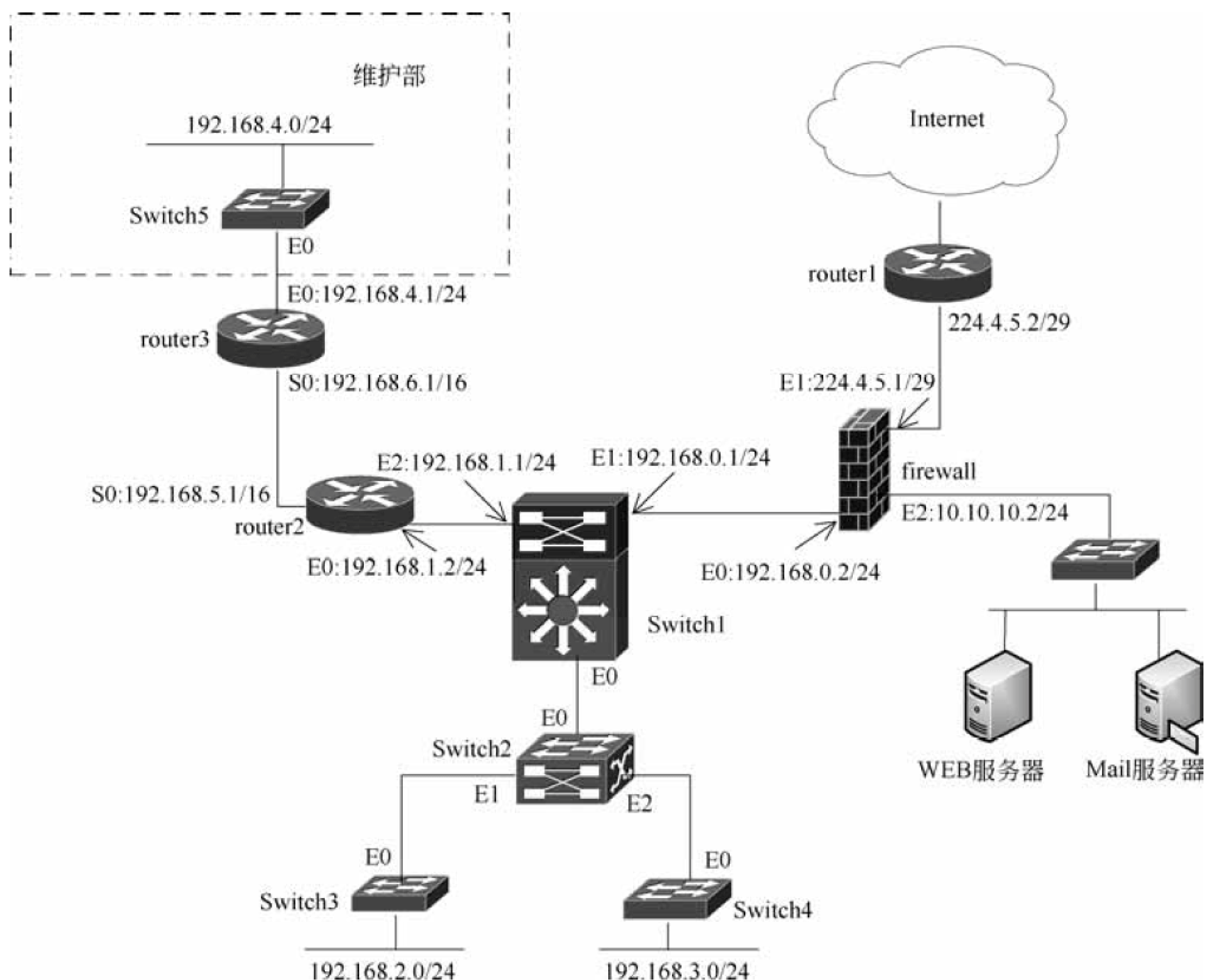



图 4-1

**【问题 1】（3 分）**

核心交换机 Switch1 的部分配置如下，请根据说明和网络拓扑图完成下列配置。

```
……
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 2
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 3
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 4
Switch1(config-if)#ip address 192.168.3.1 255.255.255.0
Switch1(config-if)#no shutdown
```

```
......
Switch1(config-router)#ip route 0.0.0.0 0.0.0.0____(1)______
Switch1(config)#ip route  (2)  255.255.255.0____(3)____
   ......
```

【问题 2】(3 分)

根据网络拓扑和需求说明，完成汇聚交换机 Switch2 的部分配置。

```
Switch2(config)#interface fastEthernet 0/0
Switch2(config-if)#switchport mode ___(4)___
Switch2(config-if)#no shutdown

Switch2(config)#interface fastEthernet 0/1
Switch2(config-if)#switchport mode ___(5)___
Switch2(config-if)#switchport access  (6)
Switch2(config-if)#no shutdown
...
```

【问题 3】(9 分)

根据网络拓扑和需求说明，完成（或解释）路由器 router2 的部分配置。

```
......
R2(config-if) # interface ethernet0
R2(config-if) # ip address___(7)___ ___(8)___
R2(config-if) # no shutdown
R2(config-if) # interface Serial0
R2(config-if) # ip address___(9)___ ___(10)___
R21(config-if) # no shutdown
...
R2(config) # ip route 0.0.0.0 0.0.0.0___(11)___
R2(config) # ip route___(12)___255.255.255.0___(13)___
R2(config) # snmp-server community public ro        //___(14)___
R2(config) # snmp-server community publicw rw       //___(15)___
......
```

【问题 4】(5 分)

按照图 4-1 所示，设置防火墙各接口 IP 地址，并根据配置说明，完成下面的命令。

```
PIX(config)#interface ethernet0 auto
PIX(config)#interface ethernet1 100full
PIX(config)#interface ethernet2 100full
PIX(config)#ip address outside ___(16)___ ___(17)___      //设置外网接口 IP
```

```
PIX(config)#ip address inside 192.168.0.2 255.255.255.0 //设置内网接口 IP
PIX(config)#ip address dmz  (18)  255.255.255.0         //设置 DMZ 接口 IP
PIX(config)#global (outside) 1 224.4.5.1-224.4.5.6
                                         //指定公网地址范围，定义地址池
PIX(config)# (19)                        //表示内网的所有主机都可以访问外网
PIX(config)#route outside 0 0  (20)      //设置默认路由
```

**试题四分析**

本题考查交换机、路由器和防火墙配置的基本知识与应用。

**【问题 1】**

本问题考查三层交换机路由的配置。根据题目说明和拓扑图可知，核心交换机的默认路由应该指向防火墙 E0 口，但是由于 DDN 通讯的要求，192.168.4.0 网段地址的路由应指向 route2 的 E0 口，所以交换机 Switch1 配置如下：

```
……
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 2
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 3
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 4
Switch1(config-if)#ip address 192.168.3.1 255.255.255.0
Switch1(config-if)#no shutdown
……
Switch1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
Switch1(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.2
    ……
```

**【问题 2】**

本问题考查交换机 vlan 的配置方法。根据题目说明和拓扑结构图，Switch2 的 E0 口上行连接核心交换机，所以该接口为 trunk 口，Switch2 的 E1 口连接 Switch3 的 E0 口，而 Switch3 的网段为 192.169.2.0，根据问题 1 可知，其 vlan 号为 vlan 3，所以 Switch2 的配置如下：

```
Switch2(config)#interface fastEthernet 0/0
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#no shutdown
```

```
Switch2(config)#interface fastEthernet 0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan3
Switch2(config-if)#no shutdown
…
```

【问题 3】

本问题考查路由器的配置。根据题目说明和拓扑图可知 R2 的各个接口地址，R2 的默认路由应该指向核心交换机 E2 口，但是由于 DDN 通讯的要求，192.168.4.0 网段地址的路由应指向 route3 的 s0 口，所以路由器 R2 配置如下：

```
R2(config-if) # interface ethernet0
R2(config-if) # ip address 192.168.1.2 255.255.255.0
R2(config-if) # no shutdown
R2(config-if) # interface Serial0
R2(config-if) # ip address 192.168.5.1 255.255.0.0
R21(config-if) # no shutdown
…
R2(config) # ip route 0.0.0.0 0.0.0.0 192.168.1.1
R2(config) # ip route 192.168.4.0 255.255.255.0 192.168.6.1
R2(config) # snmp-server community publicr ro    //设置 snmp-server 的只读团体名为 publicr
R2(config) # snmp-server community publicw rw   //设置 snmp-server 的读写团体名为 publicw
```

【问题 4】

本问题考查防火墙的配置方法。根据题目说明和拓扑结构图可知防火墙各接口 IP 地址，其默认路由应指向 route1 的接口，所以防火墙的配置如下：

```
PIX(config)#interface ethernet0 auto
PIX(config)#interface ethernet1 100full
PIX(config)#interface ethernet2 100full
PIX(config)#ip address outside 224.4.5.1 255.255.255.248//设置外网接口 IP
PIX(config)#ip address inside 192.168.0.2 255.255.255.0 //设置内网接口 IP
PIX(config)#ip address dmz 10.10.10.2 255.255.255.0      //设置 DMZ 接口 IP
PIX(config)#global (outside) 1 224.4.5.1-224.4.5.6
                                        //指定公网地址范围，定义地址池
PIX(config)# nat (inside) 1 0.0.0.0 0.0.0.0//表示内网的所有主机都可以访问外网
PIX(config)#route outside 0 0 224.4.5.2    //设置默认路由
```

## 参考答案

**【问题 1】**

（1）192.168.0.2

（2）192.168.4.0

（3）192.168.1.2

**【问题 2】**

（4）trunk

（5）access

（6）vlan 3

**【问题 3】**

（7）192.168.1.2

（8）255.255.255.0

（9）192.168.5.1

（10）255.255.0.0

（11）192.168.1.1

（12）192.168.4.0

（13）192.168.6.1

（14）设置 snmp-server 的只读团体名为 publicr

（15）设置 snmp-server 的读写团体名为 publicw

**【问题 4】**

（16）224.4.5.1

（17）255.255.255.248

（18）10.10.10.2

（19）nat (inside) 1 0 0　或　nat (inside) 1 0.0.0.0　0.0.0.0

（20）224.4.5.2

# 第 17 章　2013 上半年网络工程师上午试题分析与解答

**试题（1）**

常用的虚拟存储器由__（1）__两级存储器组成。

（1）A．主存-辅存　　B．主存-网盘　　C．Cache-主存　　D．Cache-硬盘

**试题（1）分析**

本题考查计算机系统存储系统基础知识。

在具有层次结构存储器的计算机中，虚拟存储器是为用户提供一个比主存储器大得多的可随机访问的地址空间的技术。虚拟存储技术使辅助存储器和主存储器密切配合，对用户来说，好像计算机具有一个容量比实际主存大得多的主存可供使用，因此称为虚拟存储器。虚拟存储器的地址称为虚地址或逻辑地址。

**参考答案**

（1）A

**试题（2）**

中断向量可提供__（2）__。

（2）A．I/O 设备的端口地址　　B．所传送数据的起始地址

C．中断服务程序的入口地址　　D．主程序的断点地址

**试题（2）分析**

本题考查计算机系统基础知识。

计算机在执行程序过程中，当遇到急需处理的事件时，暂停当前正在运行的程序，转去执行有关服务程序，处理完后自动返回原程序，这个过程称为中断。

中断是一种非常重要的技术，输入输出设备和主机交换数据、分时操作、实时系统、计算机网络和分布式计算机系统中都要用到这种技术。为了提高响应中断的速度，通常把所有中断服务程序的入口地址（或称为中断向量）汇集为中断向量表。

**参考答案**

（2）C

**试题（3）**

为了便于实现多级中断，使用__（3）__来保护断点和现场最有效。

（3）A．ROM　　B．中断向量表　　C．通用寄存器　　D．堆栈

**试题（3）分析**

本题考查计算机系统基础知识。

当系统中有多个中断请求时，中断系统按优先级进行排队。若在处理低级中断过程

中又有高级中断申请中断，则高级中断可以打断低级中断处理，转去处理高级中断，等处理完高级中断后再返回去处理原来的低级中断，称为中断嵌套。实现中断嵌套用后进先出的栈来保护断点和现场最有效。

**参考答案**

（3）D

**试题（4）**

DMA 工作方式下，在__（4）__之间建立了直接的数据通路。

（4）A．CPU 与外设　B．CPU 与主存　C．主存与外设　D．外设与外设

**试题（4）分析**

本题考查计算机系统基础知识。

计算机系统中主机与外设间的输入输出控制方式有多种，在 DMA 方式下，输入输出设备与内存储器直接相连，数据传送由 DMA 控制器而不是主机 CPU 控制。CPU 除了传送开始和终了时进行必要的处理外，不参与数据传送的过程。

**参考答案**

（4）C

**试题（5）、（6）**

地址编号从 80000H 到 BFFFFH 且按字节编址的内存容量为__（5）__kb，若用 16k×4bit 的存储器芯片构成该内存，共需__（6）__片。

（5）A．128　B．256　C．512　D．1024

（6）A．8　B．16　C．32　D．64

**试题（5）、（6）分析**

本题考查计算机系统基础知识。

从 80000H 到 BFFFFH 的编址单元共 3FFFF（即 $2^{18}$）个，按字节编址的话，对应的容量为 $2^8$ kb，即 256kb。若用 16k×4bit 的芯片构成该内存，构成一个 16kb 存储器需要 2 片，256÷16=16，共需要 32 片。

**参考答案**

（5）B　（6）C

**试题（7）**

王某是一名软件设计师，按公司规定编写软件文档，并上交公司存档。这些软件文档属于职务作品，且__（7）__。

（7）A．其著作权由公司享有

B．其著作权由软件设计师享有

C．除其署名权以外，著作权的其他权利由软件设计师享有

D．其著作权由公司和软件设计师共同享有

**试题（7）分析**

本题考查知识产权知识。公民为完成法人或者其他组织工作任务所创作的作品是职务作品。职务作品可以是作品分类中的任何一种形式，如文字作品、电影作品、计算机软件等。职务作品的著作权归属分两种情形：

一般职务作品的著作权由作者享有。所谓一般职务作品是指虽是为完成工作任务而为，但非经法人或其他组织主持，不代表其意志创作，也不由其承担责任的职务作品。对于一般职务作品，法人或其他组织享有在其业务范围内优先使用的权利，期限为两年。优先使用权是专有的，未经单位同意，作者不得许可第三人以与法人或其他组织使用的相同方式使用该作品。在作品完成两年内，如单位在其业务范围内不使用，作者可以要求单位同意由第三人以与法人或其他组织使用的相同方式使用，所获报酬，由作者与单位按约定的比例分配。

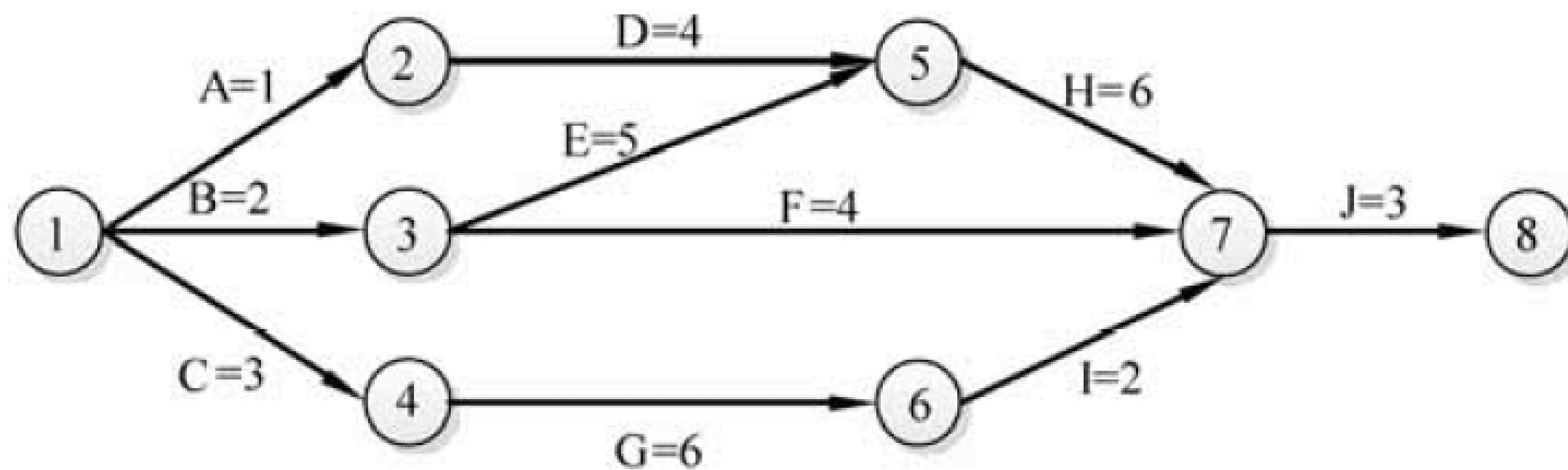
特殊的职务作品，除署名权以外，著作权的其他权利由法人或者其他组织（单位）享有。所谓特殊职务作品是指著作权法第十六条第 2 款规定的两种情况：一是主要利用法人或者其他组织的物质技术条件创作，并由法人或者其他组织承担责任的工程设计、产品设计图、计算机软件、地图等科学技术作品；二是法律、法规规定或合同约定著作权由单位享有的职务作品。

**参考答案**

（7）A

**试题（8）、（9）**

在进行进度安排时，PERT 图不能清晰地描述<u>（8）</u>，但可以给出哪些任务完成后才能开始另一些任务。某项目 X 包含任务 A、B、……、J，其 PERT 如下图所示（A=1 表示任务 A 的持续时间是 1 天），则项目 X 的关键路径是<u>（9）</u>。




（8）A．每个任务从何时开始　　B．每个任务到何时结束
　　C．各任务之间的并行情况　　D．各任务之间的依赖关系

（9）A．A-D-H-J　　B．B-E-H-J　　C．B-F-J　　D．C-G-I-J

**试题（8）、（9）分析**

本题考查项目管理及工具技术。

PERT 图可以清晰地表示各任务的开始时间和结束时间以及各任务之间的依赖关

系，但是无法很好地表示各任务之间的并行情况。

根据关键路径法，计算出题图中的关键路径为 B-E-H-J，关键路径长度为 16。

**参考答案**

（8）C　（9）B

**试题（10）**

假设某分时系统采用简单时间片轮转法，当系统中的用户数为 n、时间片为 q 时，系统对每个用户的响应时间 T=__（10）__。

（10）A．n　　B．q　　C．n×q　　D．n+q

**试题（10）分析**

在分时系统中是将把 CPU 的时间分成很短的时间片轮流地分配给各个终端用户，当系统中的用户数为 n、时间片为 q 时，那么系统对每个用户的响应时间等于 n×q。

**参考答案**

（10）C

**试题（11）**

各种联网设备的功能不同，路由器的主要功能是__（11）__。

（11）A．根据路由表进行分组转发　　B．负责网络访问层的安全

C．分配 VLAN 成员　　D．扩大局域网覆盖范围

**试题（11）分析**

网络互连设备可以根据它们工作的协议层进行分类；中继器工作于物理层；网桥和交换机工作于数据链路层；路由器工作于网络层；而网关则工作于网络层以上的协议层。

路由器根据分组中“目标网络”字段在路由表中选择匹配项，以便把分组转发到目标网络中去。通过路由器连接的局域网分属不同的子网，通过路由器互联扩大了网络的覆盖范围，但不是扩大了局域网的覆盖范围。通过在路由器中设置过滤规则可以提供网络层安全访问功能，但这不是路由器最基本、最主要的功能。而配置 VLAN 属于交换机的基本功能。

**参考答案**

（11）A

**试题（12）**

假设模拟信号的频率范围为 3～9MHz，采样频率必须大于__（12）__时，才能使得到的样本信号不失真。

（12）A．6MHz　　B．12MHz　　C．18MHz　　D．20MHz

**试题（12）分析**

根据脉冲编码调制方案，采样的频率决定了恢复的模拟信号的质量。尼奎斯特采样定理说明，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

$$f = \frac{1}{T} \geqslant 2f_{\max}$$

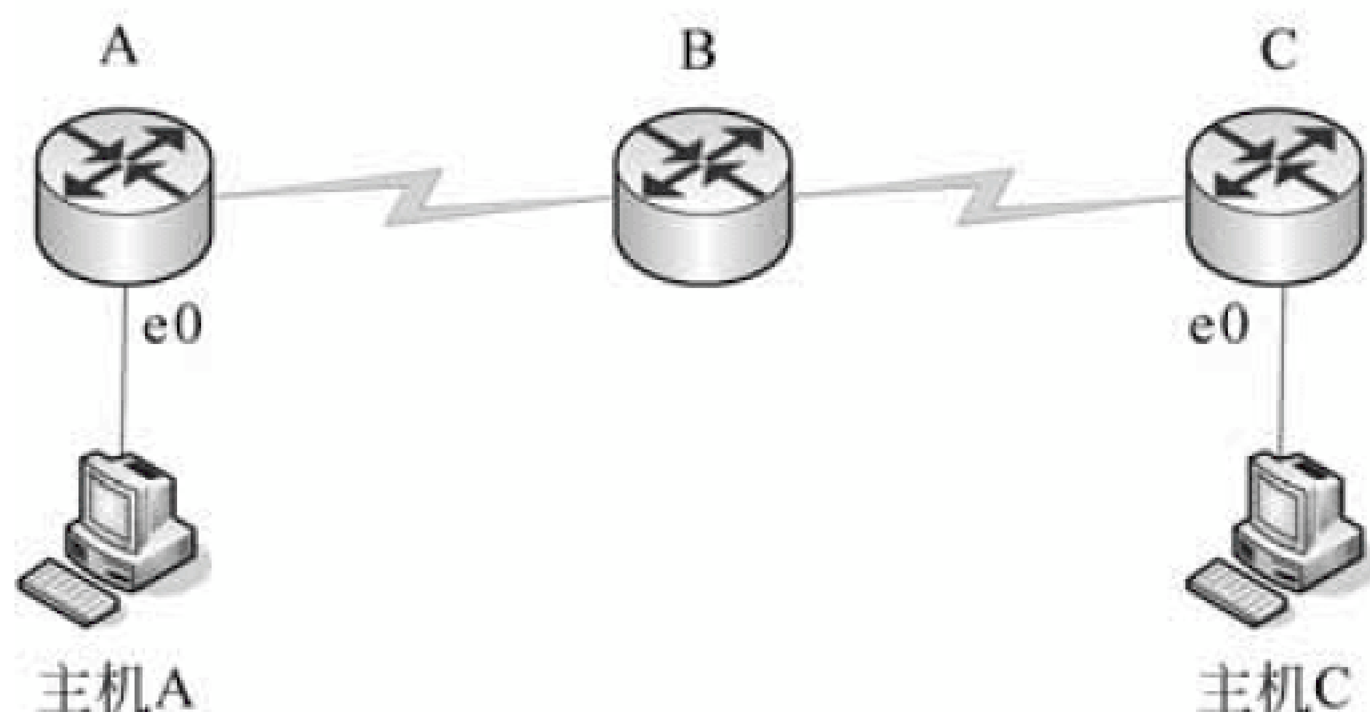
其中，$f$ 为采样频率，$T$ 为采样周期，$f_{\max}$ 为信号的最高频率。本题中信号最高频率为 9MHz，所以采样频率必须大于 18MHz。

**参考答案**

（12）C

**试题（13）**

如下图所示，若路由器 C 的 e0 端口状态为 down，则当主机 A 向主机 C 发送数据时，路由器 C 发送__（13）__。




（13）A. ICMP 回声请求报文　　B. ICMP 参数问题报文

C. ICMP 目标不可到达报文　　D. ICMP 源抑制报文

**试题（13）分析**

ICMP（Internet control Message Protocol）属于网络层协议，主要用于传送有关通信故障方面的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文有许多种，封装在 IP 数据报中传送。常见的 ICMP 报文的含义如下。

- 目标不可到达（类型 3）：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。
- 超时（类型 11）：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。
- 源抑制（类型 4）：这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。

- 参数问题（类型 12）：如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。
- 路由重定向（类型 5）：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。
- 回声（请求/响应，类型 8/0）：用于测试两个结点之间的通信线路是否畅通。收到回声请求的结点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。
- 时间戳（请求/响应，类型 13/14）：用于测试两个结点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。
- 地址掩码（请求/响应，类型 17/18）：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标结点与源结点是否在同一 LAN 中。

**参考答案**

（13）C

**试题（14）**

当一个主机要获取通信目标的 MAC 地址时，（14）。

（14）A．单播 ARP 请求到默认网关　　B．广播发送 ARP 请求
　　　C．与对方主机建立 TCP 连接　　D．转发 IP 数据报到邻居结点

**试题（14）分析**

在 Internet 中用地址分解协议（Address Resolution Protocol，ARP）来实现逻辑地址到物理地址映像，通常这种地址是与网络硬件相关的。

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td>操　作</td></tr>
<tr><td colspan="3">发送结点硬件地址</td></tr>
<tr><td colspan="3">发送结点协议地址</td></tr>
<tr><td colspan="3">目标结点硬件地址</td></tr>
<tr><td colspan="3">目标结点协议地址</td></tr>
</table>

图　ARP/RARP 分组格式

由于有两种主机地址，因而需要一种映像关系把这两种地址对应起来。ARP 分组的

格式如上图所示。

通常 Internet 应用程序把要发送的报文交给 IP 协议，IP 层实体当然知道接收方的逻辑地址，但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路层实体之前可以用两种方法得到目标物理地址：

① 查本地内存中的 ARP 地址映像表，这是本地主机已知的 IP 地址和 MAC 地址的对照表，可以由 IP 地址查找对应的 MAC 地址。

② 如果 ARP 表查不到，就广播一个 ARP 请求分组，这种分组可以到达同一子网中的所有主机和路由器。它的含义是："如果你的 IP 地址是这个分组中的目标结点协议地址，请回答你的物理地址是什么"。

③ 收到该分组的主机一方面可以用分组中的两个源地址更新自己的 ARP 地址映像表，一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的 MAC 地址，若不相符则不予回答。

④ 如果路由器知道所询问的主机的 IP 地址，则代表主机回答由以上询问，并把自己的 MAC 地址告诉发送方，后续源和目标之间的通信都是通过路由器从中转发。

**参考答案**

（14）B

**试题（15）**

路由器出厂时，默认的串口封装协议是__（15）__。

（15）A．HDLC　　B．WAP　　C．MPLS　　D．L2TP

**试题（15）分析**

路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 口。常见的网络端口有以下几种：

- RJ-45 端口：这种端口通过双绞线连接以太网。10Base-T 的 RJ-45 端口标识为"ETH"，而 100Base-TX 的 RJ-45 端口标识为"10/100bTX"。
- AUI 端口：这种端口采用 D 型 15 针连接器，用在令牌环网或总线型以太网中。路由器经 AUI 端口通过粗同轴电缆收发器连接 10Base-5 网络，也可以通过外接的 AUI-to-RJ-45 适配器连接 10Base-T 以太网。
- 高速同步串口：在路由器与广域网的连接中，应用最多的是高速同步串行口（Synchronous Serial Port），这种端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。所以默认的封装协议是 HDLC。
- ISDN BRI 端口：ISDN BRI 端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 端口采用 RJ-45 标准，与 ISDN NT1 的连接使用 RJ-45-to-RJ-45 直通线。
- 异步串口：异步串口（ASYNC）主要应用于与 Modem 或 Modem 池的连接，以实现远程计算机通过 PSTN 拨号接入。异步端口的速率不是很高，也不要求同步

传输。

- Console 端口：Console 端口通过专用电缆连接至计算机串行口，利用终端仿真程序对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。
- AUX 端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Prot）。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行转换。AUX 端口支持硬件流控。

**参考答案**

（15）A

**试题（16）**

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，每秒钟传送 100 个字符，则有效数据速率为__（16）__。

（16）A．100b/s　　B．500b/s　　C．700b/s　　D．1000b/s

**试题（16）分析**

异步通信方案是把字符作为同步的单位，字符之间插入少量的同步信息。面向字符的同步协议依赖于具体的字符编码，不同字符编码的系统之间不能通信。按照本题意说明，每秒传送 100 个字符，每个字符中的有效信息占 7/11，所以有效数据速率为 11×100×7/11=700b/s。

**参考答案**

（16）C

**试题（17）**

下列选项中，不采用虚电路通信的网络是__（17）__网。

（17）A．X.25　　B．帧中继　　C．ATM　　D．IP

**试题（17）分析**

X.25 网络是早期的公用数据网，在网络层通过虚电路提供面向连接的服务。帧中继是对 X.25 网络的改进，在数据链路层建立虚电路连接，同时也简化了差错控制功能，以适应高速光纤通信的需要。ATM 是为综合业务数字网开发的传输技术，在网络层建立虚电路连接，以 53 字节的信元为传输的单位。以上三种网络都是电信部门开发的网络通信技术，继承了早期电话网络面向连接的通信模式。IP 协议是在因特网中使用的网络层协议，当初设计时为了适应军事通信的需要，采用了无连接的通信方案。在 IP 网络中，每个数据报都是独立传送的，所有的协议数据单元到达目标后需要进行纠错和重新排序，才能提交给上层实体。

**参考答案**

（17）D

**试题（18）**

在网络层采用分层编址方案的好处是＿（18）＿。

（18）A．减少了路由表的长度

B．自动协商数据速率

C．更有效地使用 MAC 地址

D．可以采用更复杂的路由选择算法

**试题（18）分析**

在网络层采用分层的编址方案可以把网络分成大小不等的多级网络，即大网络中包含小网络。不同层级的网络路由器提供的路由信息的繁简程度不同。这样，上一级网络路由器的路由表就可以得到简化，只有子网内部的路由器才指向具体的目标主机。

**参考答案**

（18）A

**试题（19）**

在交换网络中，VTP 协议的作用是什么？＿（19）＿。

（19）A．选举根网桥

B．将 VLAN 信息传播到整个网络

C．建立端到端连接

D．选择最佳路由

**试题（19）分析**

VLAN 中继协议（VLAN Trunking Protocol，VTP）是 Cisco 公司的专利协议。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为 3 种：

① 服务器模式（Server）：交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

② 客户机模式（Client）：在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

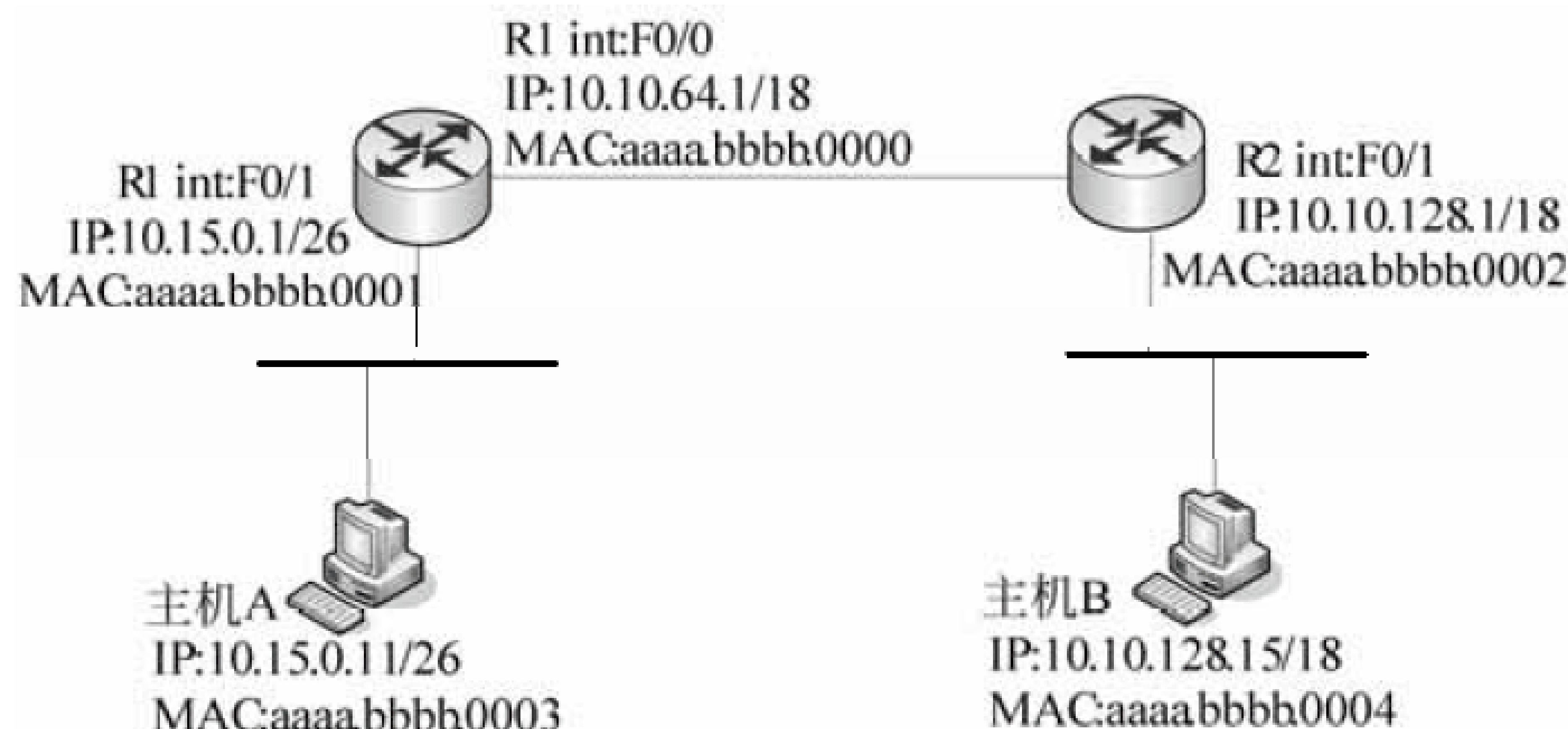
③ 透明模式（Transparent）：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

**参考答案**

（19）B

**试题（20）**

参见下图，主机 A ping 主机 B，当数据帧到达主机 B 时，其中包含的源 MAC 地址和源 IP 地址是__（20）__。




（20）A．aaaa.bbbb.0003 和 10.15.0.11

B．aaaa.bbbb.0002 和 10.10.128.1

C．aaaa.bbbb.0002 和 10.15.0.11

D．aaaa.bbbb.0000 和 10.10.64.1

**试题（20）分析**

主机 A 发出的 ping 报文经过路由器 R1 和 R2 转发，到达主机 B 时，根据 ARP 协议代理机制，其中包含的源 MAC 地址是 R2 的 MAC 地址——aaaa.bbbb.0002。当然，源 IP 地址还是主机 A 的 IP 地址 10.15.0.11。

**参考答案**

（20）C

**试题（21）**

下面的描述中，不属于链路状态路由协议的特点是__（21）__。

（21）A．提供了整个网络的拓扑视图

B．计算到达各个目标的最短通路

C．邻居结点之间互相交换路由表

D．具有事件触发的路由更新功能

**试题（21）分析**

执行链路状态路由协议的路由器只保留自己知道的部分网络的拓扑信息，但是所有路由器保存的路由信息的总和则可以提供整个网络的拓扑结构视图。各个链路状态路由器根据自己的路由表计算到达目标的最短通路。链路状态路由协议在网络拓扑结构改变时触发路由更新功能。执行链路状态协议的路由器通过 Hello 协议来发现邻居，并在其邻居中选择需要交换链路状态信息的路由器，与之建立毗邻关系（Adjacency）。并不是每一对邻居都需要交换路由信息，因而也不是每一对邻居都要建立毗邻关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器（Designated Router，DR），其他的路由

器都与DR建立毗邻关系，把自己掌握的链路状态信息提交给DR，由DR代表这个网络向外界发布。

**参考答案**

（21）C

**试题（22）**

关于网桥和交换机，下面的描述中正确的是__（22）__。

（22）A．网桥端口数少，因而比交换机转发更快

B．网桥转发广播帧，而交换机不转发广播帧

C．交换机是一种多端口网桥

D．交换机端口多，因而扩大了冲突域的大小

**试题（22）分析**

网桥和交换机都是第二层转发设备，即都是根据数据链路层地址转发（包括广播）数据包。二者的区别是网桥的端口数较少，一般是用主机插入多个网卡来连接多个子网，并通过软件来实现分组过滤功能。而交换机通常是采用专门的硬件实现，端口数较多。由于采用了专用硬件，因此交换机转发速度更快。无论网桥或交换机，一个端口就是一个冲突域。

**参考答案**

（22）C

**试题（23）**

使用路由器对局域网进行分段的好处是__（23）__。

（23）A．广播帧不会通过路由进行转发

B．通过路由器转发减少了通信延迟

C．路由器的价格便宜，比使用交换机更经济

D．可以开发新的应用

**试题（23）分析**

路由器是第三层设备，它不转发第二层广播帧。所以使用路由器对局域网进行分段的好处是可以隔离第二层广播风暴，减少了冲突域的范围。

**参考答案**

（23）A

**试题（24）**

OSPF网络可以划分为多个区域（area），下面关于区域的描述中错误的是__（24）__。

（24）A．区域可以被赋予0～65535中的任何编号

B．单域OSPF网络必须配置成区域1

C．区域0被称为主干网

D．分层的OSPF网络必须划分为多个区域

**试题（24）分析**

OSPF 网络可以划分为多个区域（area），每个 OSPF 区域被指定了一个 32 位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为 0.0.0.0。单域 OSPF 网络就是只有主干区域的网络（配置成区域 0）。分层的 OSPF 网络必须划分为多个区域。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

- 标准区域：可以接收任何链路更新信息和路由汇总信息。
- 主干区域：是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。
- 存根区域：不接收本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。
- 完全存根区域：不接收自治系统以外的路由信息，也不接收自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。
- 不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（24）B

**试题（25）**

与 RIPv1 相比，RIPv2 的改进是__（25）__。

（25）A．采用了可变长子网掩码

B．使用 SPF 算法计算最短路由

C．广播发布路由更新信息

D．采用了更复杂的路由度量算法

**试题（25）分析**

RIP 分为两个版本。RIPv1（RFC 1058，1988）是早期的路由协议，使用本地广播地址 255.255.255.255 发布路由信息，默认的路由更新周期为 30 秒，持有时间（Hold-Down Time）为 180 秒。RIP 以跳步计数（hop count）来度量路由费用，显然这不是最好的度量标准。例如，若有两条到达同一目标的连接，一条是经过两跳的 10Mb 以太网连接，另一条是经过一跳的 64kbWAN 连接，则 RIP 会选取 WAN 连接作为最佳路由。在 RIP 协议中，15 跳是最大跳数，16 跳是不可到达网络，经过 16 跳的任何分组将被路由器丢弃。

RIPv1 是有类别的协议，这意味着配置 RIPv1 时必须使用 A、B 或 C 类 IP 地址和子网掩码，例如不能把子网掩码 255.255.255.0 用于 B 类网络 172.16.0.0。

对于同一目标，RIP 路由表项中最多可以有 6 条等费用的通路，虽然默认是 4 条。RIP 可以实现等费用通路的负载均衡（equal-cost load balancing），这种机制提供了链路

冗余功能，以对付可能出现的连接失效，但是 RIP 不支持不等费用通路的负载均衡。

RIPv2 是增强了的 RIP 协议，定义在 RFC 1721 和 RFC 1722（1994）中。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update）机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是 RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制路由更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

**参考答案**

（25）A

**试题（26）、（27）**

把网络 117.15.32.0/23 划分为 117.15.32.0/27，则得到的子网是多少个？__（26）__。每个子网中可使用的主机地址是多少个？__（27）__。

（26）A. 4　　B. 8　　C. 16　　D. 32

（27）A. 30　　B. 31　　C. 32　　D. 34

**试题（26）、（27）分析**

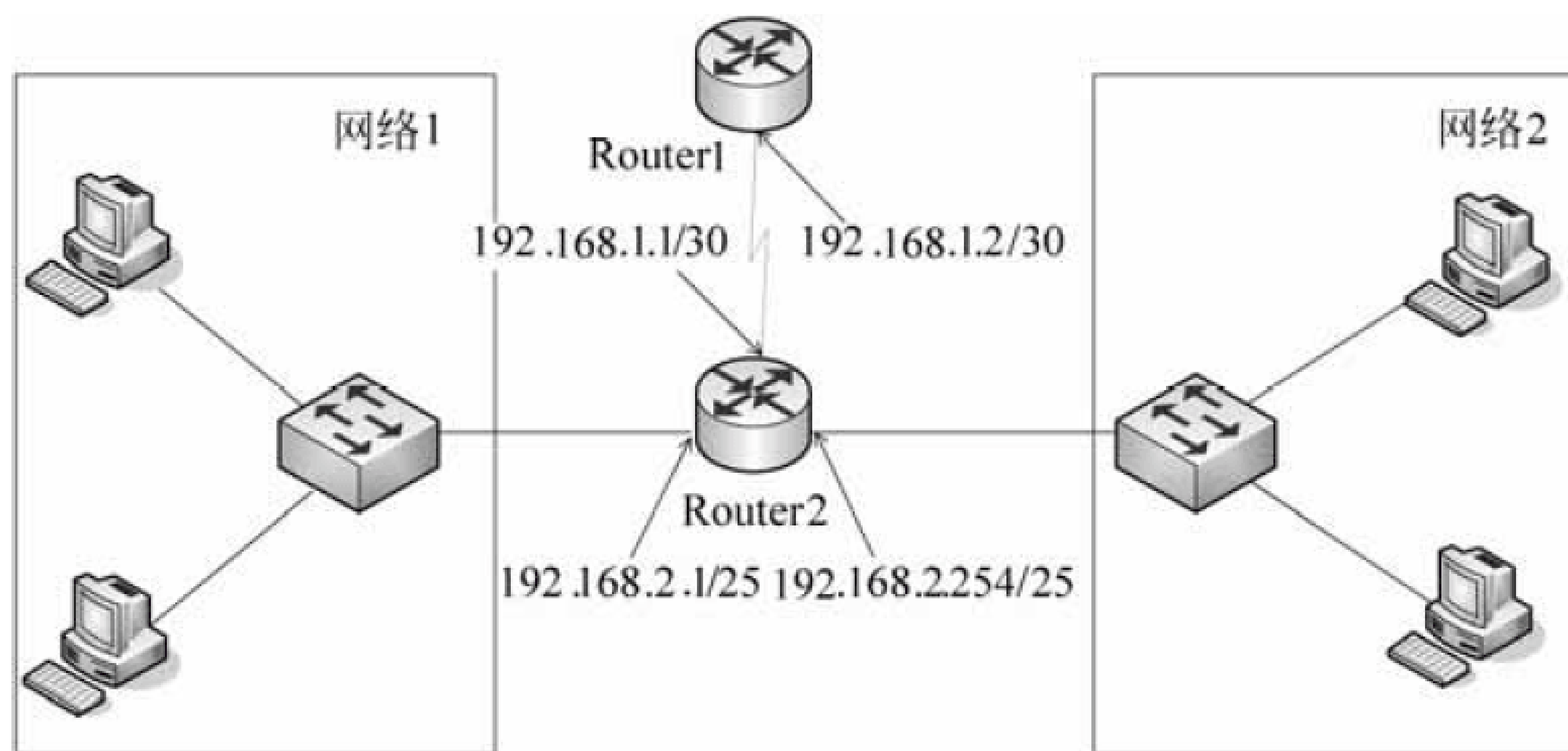
把网络 117.15.32.0/23 划分为 117.15.32.0/27，则子网掩码扩大了 4 位，所以得到的子网是 16 个。由于子网掩码为 27 位，所以主机地址只占 5 位，每个子网中可使用的主机地址是 30 个。

**参考答案**

（26）C　（27）A

**试题（28）～（30）**

网络配置如下图所示，为路由器 Router1 配置访问网络 1 和网络 2 的命令是__（28）__。路由配置完成后，在 Router1 的__（29）__可以查看路由，查看路由采用的命令是__（30）__。



（28）A．ip　route　192.168.2.0　255.255.255.0　192.168.1.1

B．ip　route　192.168.2.0　255.255.255.128　192.168.1.2

C．ip　route　192.168.1.0　255.255.255.0　192.168.1.1

D．ip　route　192.168.2.128　255.255.255.128　192.168.1.2

（29）A．仅 Router1#模式下

B．Router1>或 Router1#模式下

C．Router1(config)# 模式下

D．Router1(config-if)# 模式下

（30）A．config/all　　B．route display　　C．show ip route　　D．show route

**试题（28）～（30）分析**

本题考查路由器配置及相关命令、模式。

在路由器 Router1 上配置一条记录即可访问网络 1 和网络 2，网络 1 和网络 2 汇聚后的地址为 192.168.2.0/24，下一跳地址为 192.168.1.1，故配置命令为 ip　route　192.168.2.0　255.255.255.0　192.168.1.1。

路由器中，Router1>或 Router1#模式下均可查看路由，查看的命令为 show ip route。

**参考答案**

（28）A　（29）B　（30）C

**试题（31）**

有多种方案可以在一台服务器中安装 Windows 和 Linux 两种网络操作系统，其中可以同时运行 Windows 和 Linux 系统的方案是（31）。

（31）A．GRUB 多引导程序　　B．LILO 多引导程序

C．VMWare 虚拟机　　D．Windows 多引导程序

**试题（31）分析**

本题考查网络操作系统安装和引导的基础知识。

在一台服务器中安装 Windows 和 Linux 两种网络操作系统，可以有多种方案，选项 A、B、C 和 D 都是可行方案。但 A、B 和 D 三个选项使用的都是多引导程序，每次运行只能从 Windows 和 Linux 两个系统中选择一个运行，如果需要同时运行 Windows 和 Linux 系统则只能选用虚拟机方案。

**参考答案**

（31）C

**试题（32）**

Linux 系统中的文件操作命令 grep 用于（32）。

（32）A．列出文件的属性信息　　B．在指定路径查找文件

C．复制文件　　D．在指定文件中查找指定的字符串

**试题（32）分析**

本题考查 Linux 系统下的常用命令。

linux 系统中常用的文件操作命令有 ls、find、cp、grep 等。

ls 命令将每个由 Directory 参数指定的目录或者每个由 File 参数指定的名称写到标准输出，以及所要求的和标志一起的其他信息。如果不指定 File 或 Directory 参数，ls 命令显示当前目录的内容。

find 将文件系统内符合 expression 的文件列出来。可以指定文件的名称、类别、时间、大小、权限等不同信息的组合，只有完全相符的文件才会被列出来。

cp 命令的功能是将给出的文件或目录拷贝到另一文件或目录中。

grep（global search regular expression(RE) and print out the line，全面搜索正则表达式并把行打印出来）是一种强大的文本搜索工具，它能使用正则表达式搜索文本，并把匹配的行打印出来。

**参考答案**

（32）D

**试题（33）**

在某台主机上无法访问域名为 www.bbb.cn 的网站，而局域网中的其他主机可正常访问，在该主机上执行 ping 命令时有如下所示的信息：

```
C:\>ping www.bbb.cn
Pinging www.bbb.cn [202.112.0.36] with 32 bytes of data:
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Ping statistics for 202.112.0.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

分析以上信息，可能造成该现象的原因是__（33）__。

（33）A．该计算机设置的 DNS 服务器工作不正常

B．该计算机的 TCP/IP 协议工作不正常

C．该计算机连接的网络中相关网络设备配置了拦截的 ACL 规则

D．该计算机网关地址设置错误

**试题（33）分析**

本题考查 Internet 的综合运用。

采用 ping www.bbb.com 命令得到目的 IP 地址不可达的结果，首先可排除 DNS 服务器不正常这一选项；如果 TCP/IP 协议工作不正常，或计算机网关地址设置错误，也都不

可能得到域名的正确解析，因此只可能是在防火墙或相关设备上进行了规则设置。

**参考答案**

（33）C

**试题（34）**

近年来，在我国出现的各类病毒中，__（34）__病毒通过木马形式感染智能手机。

（34）A．欢乐时光　B．熊猫烧香　C．X 卧底　D．CIH

**试题（34）分析**

本题考查病毒及其危害。

欢乐时光及熊猫烧香均为蠕虫病毒，CIH 则为系统病毒，这 3 者均以感染台式机或服务器为主，且产生较早；X 卧底则是新近产生的、通过木马形式传播、目标为智能手机的病毒。

**参考答案**

（34）C

**试题（35）**

某 DHCP 服务器设置的 IP 地址池从 192.168.1.100 到 192.168.1.200，此时该网段下某台安装 Windows 系统的工作站启动后，获得的 IP 地址是 169.254.220.188，导致这一现象最可能的原因是__（35）__。

（35）A．DHCP 服务器设置的租约期太长

B．DHCP 服务器提供了保留的 IP 地址

C．网段内还有其他的 DHCP 服务器，工作站从其他的服务器上获得的地址

D．DHCP 服务器没有工作

**试题（35）分析**

本题考查 DHCP 服务器及 DHCP 协议的工作原理。

Windows 系统中，获得的 IP 地址是 169.254.220.188，表明 DHCP 服务器没有工作，系统给客户机自行分配了一个 169 段的地址。

**参考答案**

（35）D

**试题（36）**

下列关于 DHCP 的说法中，错误的是__（36）__。

（36）A．Windows 操作系统中，默认租约期是 8 天

B．客户机通常选择最先响应的 DHCP 服务器提供的地址

C．客户机可以跨网段申请 DHCP 服务器提供的 IP 地址

D．客户机一直使用 DHCP 服务器分配给它的 IP 地址，直至租约期结束才开始请求更新租约

**试题（36）分析**

本题考查 DHCP 协议及服务器的配置。

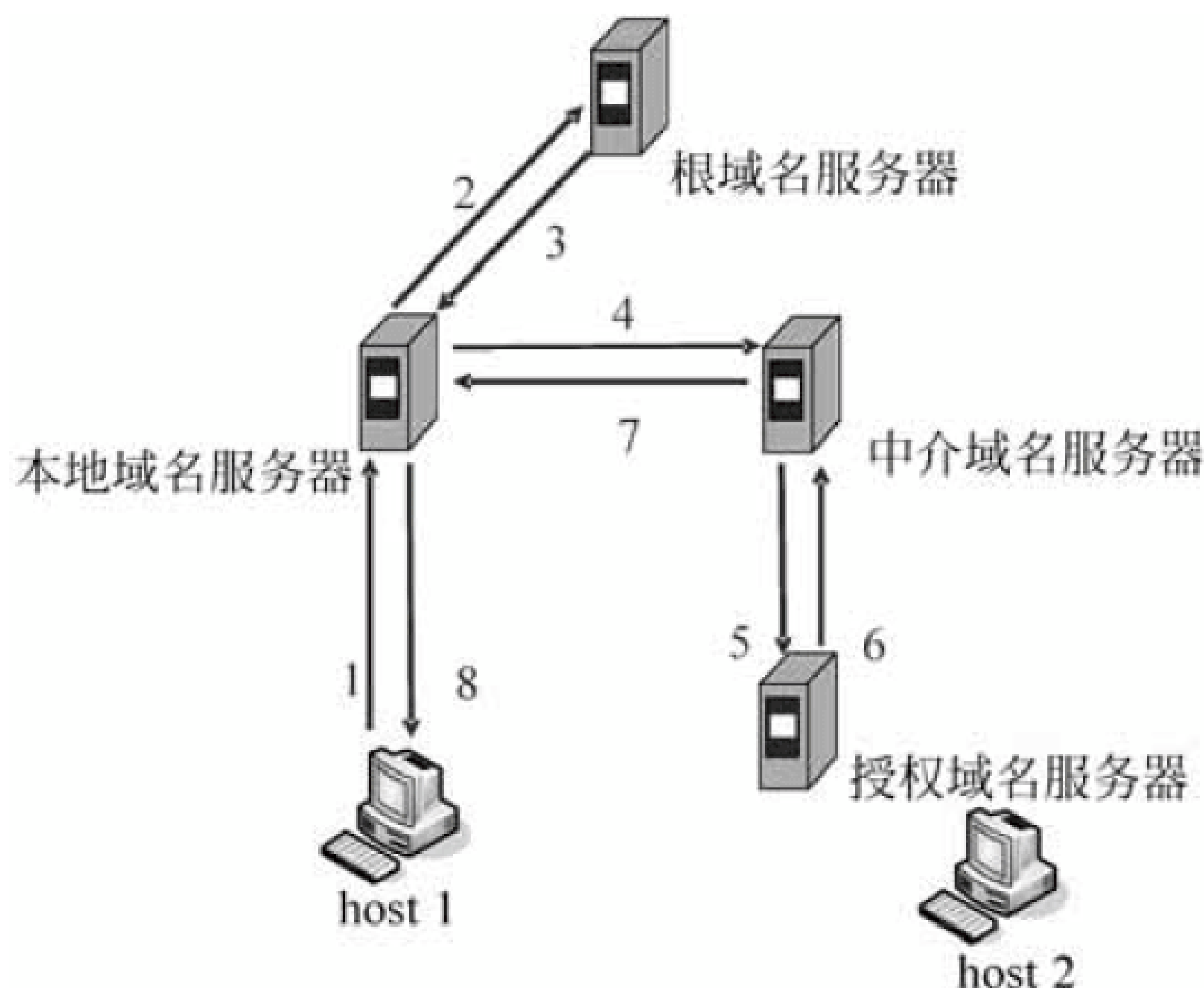
Windows 操作系统中，DHCP 提供的 IP 地址的默认租约期是 8 天；在有多个 DHCP 服务器响应时，客户机通常选择最先响应的 DHCP 服务器提供的地址；客户机可以通过中继代理跨网段申请 DHCP 服务器提供的 IP 地址；客户机一直使用 DHCP 服务器分配给它的 IP 地址，在租约期 50%时开始请求更新租约。

**参考答案**

（36）D

**试题（37）**

主机 host1 对 host2 进行域名查询的过程如下图所示，下列说法中正确的是__（37）__。




（37）A. 根域名服务器采用迭代查询，中介域名服务器采用递归查询
B. 根域名服务器采用递归查询，中介域名服务器采用迭代查询
C. 根域名服务器和中介域名服务器均采用迭代查询
D. 根域名服务器和中介域名服务器均采用递归查询

**试题（37）分析**

本试题考查域名服务器进行域名解析时的查询方法。

DNS 客户端都配置了一个或多个 DNS 服务器的地址，无论是静态或动态配置的，这些 DNS 服务器都是用户所在域的授权服务器，而用户主机则是该域的成员。当用户在浏览器地址栏输入一个域名时，客户端就可以向本地的 DNS 服务器发出查询请求。查询过程分为两种查询方式：

① 递归查询：当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果——IP 地址或错误信息。如果查询请求在本地服务器中不能完成，那么服务器就根据它的配置向域名树中的上级服务器进行查询，在最坏的情况下可能要查询到根服务器。每次查询返回的结果如果是其他名字服务器的 IP 地址，则本地服务器要把查询请求发送给这些服务器做进一步的查询。

② 迭代查询：服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器得到的响应可能不是目标的 IP 地址，而是其他服务器的引用（名字和地址），那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的 IP 地址或错误信息。

因此，根域名服务器采用迭代查询，中介域名服务器采用递归查询。

**参考答案**

（37）A

**试题（38）**

网络拓扑设计对网络的影响主要表现在（38）。

① 网络性能　② 系统可靠性　③ 出口带宽　④ 网络协议

（38）A. ①、②　B. ①、②、③

C. ③、④　D. ①、②、④

**试题（38）分析**

本题考查网络规划与设计，以及网络拓扑结构等知识。

网络拓扑结构不同，对网络的性能、系统可靠性、网络协议的选择均会造成影响；出口带宽与 ISP 提供的容量有关，与内部网络结构的设计无关。

**参考答案**

（38）D

**试题（39）**

如果一台 cisco PIX 防火墙有如下的配置：

```
PIX(config)#nameif ethernet0 f1 security0
PIX(config)#nameif ethernet1 f2 security100
PIX(config)#nameif ethernet2 f3 security50
```

那么，以下说法中正确的是（39）。

（39）A. 端口 f1 作为外部网络接口，f2 连接 DMZ 区域，f3 作为内部网络接口

B. 端口 f1 作为内部网络接口，f2 连接 DMZ 区域，f3 作为外部网络接口

C. 端口 f1 作为外部网络接口，f2 作为内部网络接口，f3 连接 DMZ 区域

D. 端口 f1 作为内部网络接口，f2 作为外部网络接口，f3 连接 DMZ 区域

**试题（39）分析**

本题考查 cisco PIX 防火墙的安全级别设置。

cisco PIX 防火墙中，给定的数字越大说明安全级别越高。在网络中，外部网络安全级别最低，其次是 DMZ 区，内部网络接口最高。

**参考答案**

（39）C

**试题（40）**

在接收邮件时，客户端代理软件与 POP3 服务器通过建立__（40）__连接来传送报文。

（40）A. UDP　　B. TCP　　C. P2P　　D. DHCP

**试题（40）分析**

本题考查电子邮件及相关应用。

在接收邮件时，客户端代理软件与 POP3 服务器通过建立 TCP 连接来传送报文。

**参考答案**

（40）B

**试题（41）**

利用三重 DES 进行加密，以下说法正确的是__（41）__。

（41）A. 三重 DES 的密钥长度是 56 位

B. 三重 DES 使用三个不同的密钥进行三次加密

C. 三重 DES 的安全性高于 DES

D. 三重 DES 的加密速度比 DES 加密速度快

**试题（41）分析**

本题考查三重 DES 的知识。

三重 DES 是 DES 的改进算法，它使用两把密钥对报文作三次 DES 加密，效果相当于将 DES 密钥的长度加倍了，克服了 DES 密钥长度较短的缺点。本来，应该使用三个不同的密钥进行三次加密，这样就可以把密钥的长度加长到 3×56=168 位。但许多密码设计者认为 168 位的密钥已经超过实际需要了，所以便在第一层和第三层中使用相同的密钥，产生一个有效长度为 112 位的密钥。之所以没有直接采用两重 DES，是因为第二层 DES 不是十分安全，它对一种称为“中间可遇”的密码分析攻击极为脆弱，所以最终还是采用了利用两个密钥进行三重 DES 加密操作。这种方法的缺点是要花费原来三倍的时间，但从另一方面来看，三重 DES 的 112 位密钥长度是很“强壮”的加密方式了。

**参考答案**

（41）C

**试题（42）**

利用报文摘要算法生成报文摘要的目的是__（42）__。

（42）A. 验证通信对方的身份，防止假冒

B. 对传输数据进行加密，防止数据被窃听

C. 防止发送方否认发送过的数据

D. 防止发送的报文被篡改

**试题（42）分析**

本题考查报文摘要的知识。

报文摘要是指单向哈希函数算法将任意长度的输入报文经计算得出固定位的输出。报文摘要是用来保证数据完整性的。传输的数据一旦被修改那么计算出的摘要就不同，只要对比两次摘要就可确定数据是否被修改过。

**参考答案**

（42）D

**试题（43）**

（43）是支持电子邮件加密服务的协议。

（43）A．PGP　　B．PKI　　C．SET　　D．Kerberos

**试题（43）分析**

本题考查电子邮件加密服务的知识。

PKI 即公钥基础设施，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

SET 即安全电子交易协议，是美国 Visa 和 MasterCard 两大信用卡组织等联合于 1997 年 5 月 31 日推出的用于电子商务的行业规范，其实质是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范，目的是为了保证网络交易的安全。

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。

PGP 是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。

**参考答案**

（43）A

**试题（44）**

下面能正确 sss 表示 L2TP 数据包的封装格式的是（44）。

（44）

A.

| IP | TCP | L2TP | PPP |
|---|---|---|---|

B.

| IP | UDP | L2TP | PPP |
|---|---|---|---|

C.

| IP | L2TP | TCP | PPP |
|---|---|---|---|

D.

| IP | L2TP | UDP | PPP |
|---|---|---|---|

**试题（44）分析**

本题考查 L2TP 数据包的基本知识。

第 2 层隧道协议（Layer 2 Tunneling Protocol，L2TP）用于把各种拨号服务集成到 ISP 的服务提供点。L2TP 扩展了 PPP 模型，允许第二层连接端点和 PPP 会话端点驻在由分组交换网连接的不同的设备中。

L2TP 报文分为控制报文和数据报文。控制报文用于建立、维护和释放隧道和呼叫。数据报文用于封装 PPP 帧，以便在隧道中传送。控制报文使用了可靠的控制信道以保证提交，数据报文被丢失后不再重传。

在 IP 网上使用 UDP 和一系列的 L2TP 消息对隧道进行维护，同时使用 UDP 将 L2TP 封装的 PPP 帧通过隧道发送。可以对封装的 PPP 帧中的负载数据进行加密或压缩。下图为一个 L2TP 数据包格式。

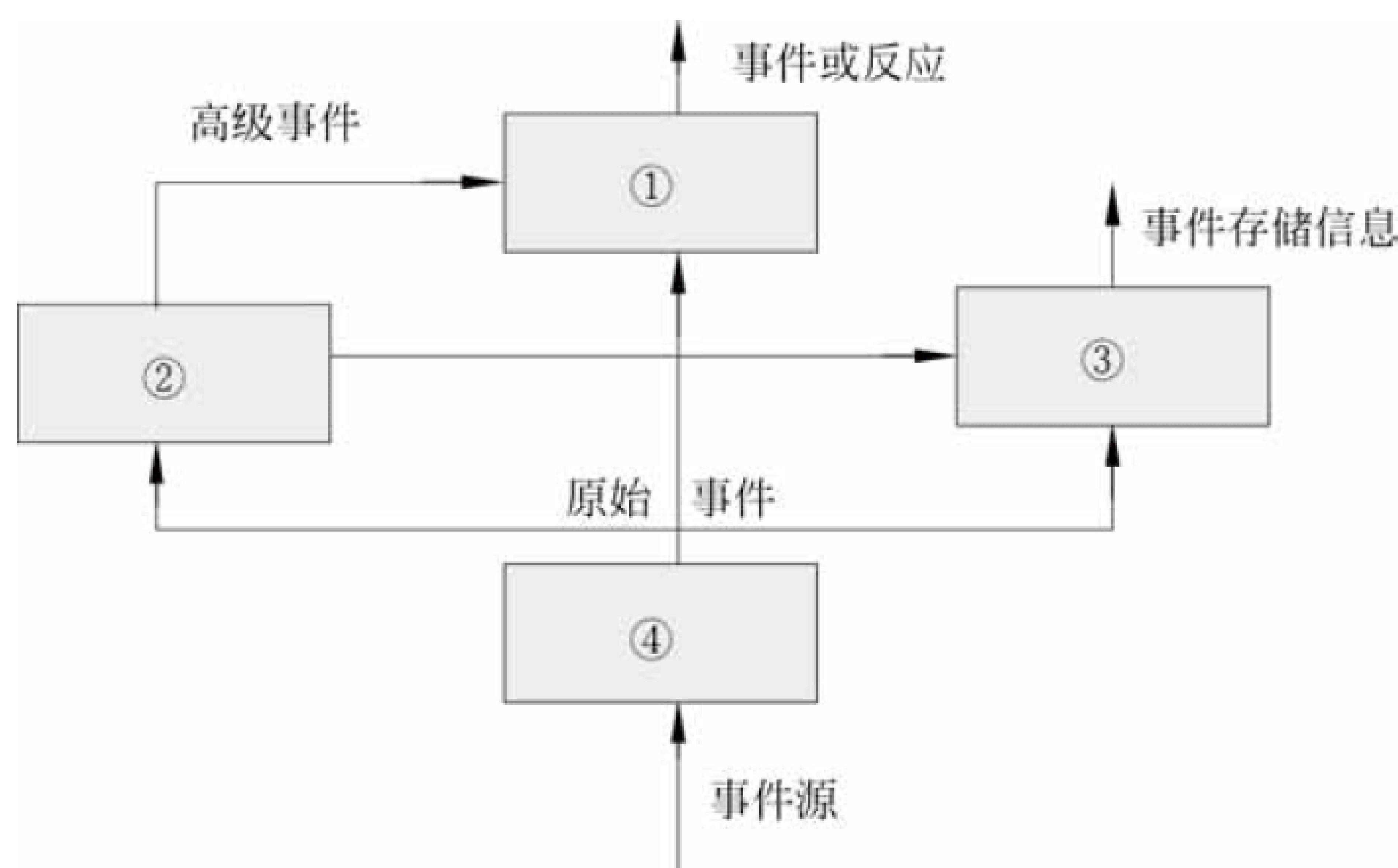



**参考答案**

（44）B

**试题（45）**

下图为 DARPA 提出的公共入侵检测框架示意图，该系统由 4 个模块组成。其中模块①～④对应的正确名称为__（45）__。




（45）A．事件产生器、事件数据库、事件分析器、响应单元

B．事件分析器、事件产生器、响应单元、事件数据库

C．事件数据库、响应单元、事件产生器、事件分析器

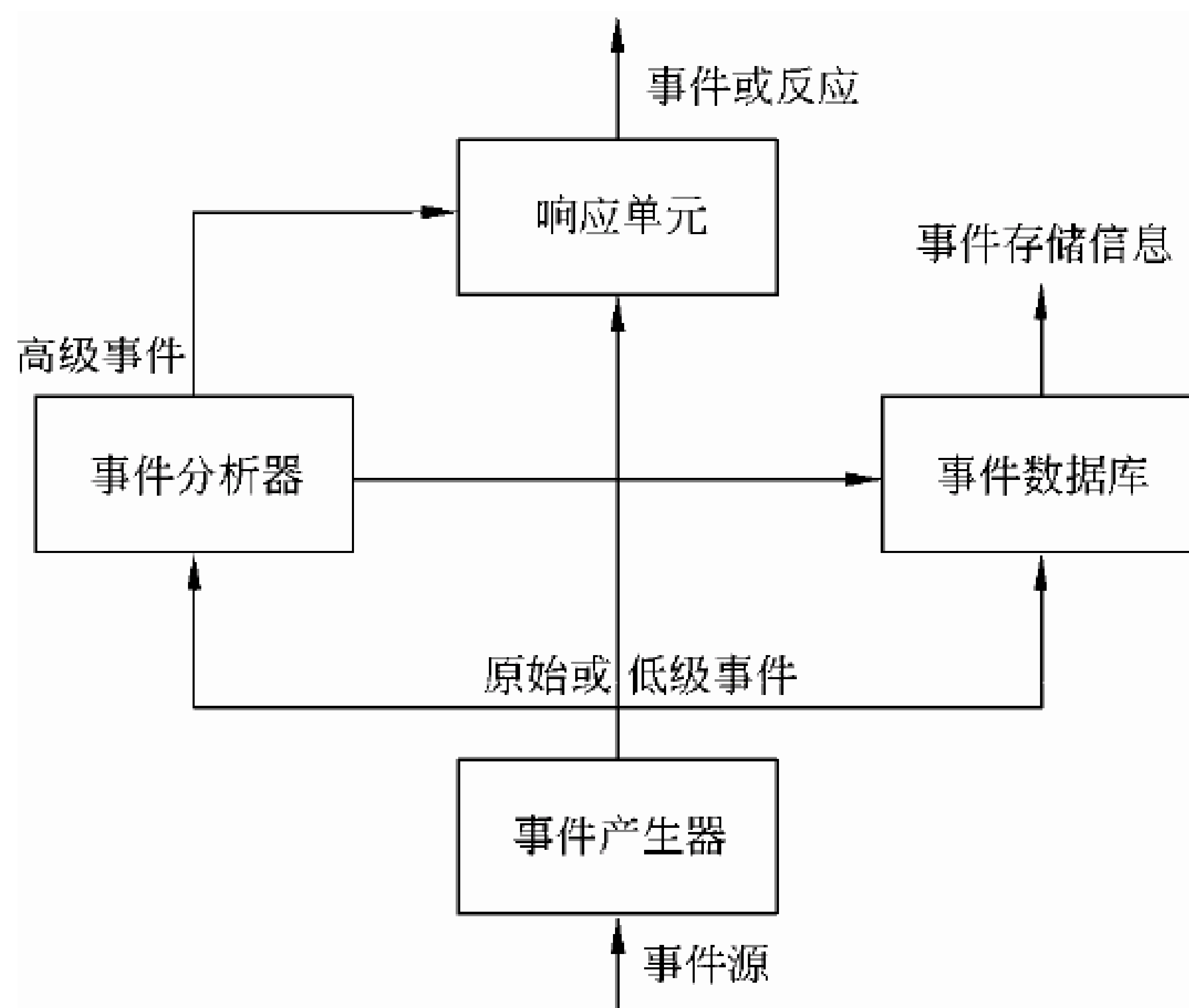
D．响应单元、事件分析器、事件数据库、事件产生器

**试题（45）分析**

本题考查入侵检测的知识。

美国国防部高级研究计划局（DARPA）提出的公共入侵检测框架（Common Intrusion

Detection Framework，CIDF）由 4 个模块组成（如下图所示）。




① 事件产生器（Event generators，E-boxes）。负责数据的采集，并将收集到的原始数据转换为事件，向系统的其他模块提供与事件有关的信息。

② 事件分析器（Event Analyzers，A-boxes）。接收事件信息并对其进行分析，判断是否为入侵行为或异常现象。

③ 事件数据库（Event DataBases，D-boxes）。存放有关事件的各种中间结果和最终数据的地方，可以是面向对象的数据库，也可以是一个文本文件。

④ 响应单元（Response units，R-boxes）。根据报警信息做出各种反应，强烈的反应就是断开连接、改变文件属性等，简单的反应就是发出系统提示，引起操作人员注意。

**参考答案**

（45）D

**试题（46）**

在 Windows Server 2003 中，创建用户组时，可选择的组类型中，仅用于分发电子邮件且没有启用安全性的是__（46）__。

（46）A. 安全组　　B. 本地组　　C. 全局组　　D. 通信组

**试题（46）分析**

在 Windows Server 2003 中创建域组时，在“组类型”选项区域中可选择组的类型：

安全组。可以显示在随机访问控制列表（DACL）中的组，该列表用于定义对资源和对象的权限。“安全组”也可用作电子邮件实体，给这种组发送电子邮件的同时也会将该邮件发给组中的所有成员。

通信组。仅用于分发电子邮件并且没有启用安全性的组。不能将“通信组”显示在用于定义资源和对象权限的随机访问控制列表（DACL）中。“通信组”只能与电子邮件应用程序（例如，Microsoft Exchange）一起使用，以便将电子邮件发送到用户集合。如果因为安全目的并不需要组，可以选择创建“通信组”而不要创建“安全组”。

**参考答案**

（46）D

**试题（47）**

在 Window Server 2003 中，与 Window Server 2000 终端服务对应的是__（47）__。

（47）A．远程协助　　B．管理远程桌面
C．远程管理的 Web 界面　　D．远程安装服务

**试题（47）分析**

本题考查 Window Server 2003 中有关终端服务的新特性。

Windows Server 2003 终端服务添加了管理远程桌面，它实际上是所有服务器版本的远程管理模式，无需像 Windows 2000 那样一定要 Windows 2000 Server CD 才能安装它，只需进入远程选项卡，就可以在所有服务器版本中打开远程桌面。

**参考答案**

（47）B

**试题（48）**

网络管理系统由网络管理站、网管代理、网络管理协议和管理信息库 4 个要素组成。当网管代理向管理站发送异步事件报告时，使用的操作是__（48）__。

（48）A．get　　B．get-next　　C．trap　　D．set

**试题（48）分析**

本题考查网络管理中 SNMP 协议支持的服务原语。

Get 检索数据，Set 改变数据，GetNext 提供扫描 MIB 树和连续检索数据的方法，Trap 则提供从代理进程到管理站的异步报告机制。

**参考答案**

（48）C

**试题（49）**

在 MIB-2 中，IP 组对象 ipInReceives 为接收的 IP 数据报总数，其数据类型为__（49）__类型。

（49）A．整数　　B．计数器　　C．序列　　D．计量器

**试题（49）分析**

本题考查 SNMP 协议中 MIB-2 的功能组对象的数据类型。

在 MIB-2 中，IP 组对象 ipInReceives 为接收的 IP 数据报总数，其数据类型为计数器类型（Counter）。

**参考答案**

（49）B

**试题（50）**

在 TCP/IP 协议分层结构中，SNMP 是在__（50）__协议之上的异步请求/响应协议。

（50）A．TCP　　B．UDP　　C．HTTP　　D．P2P

**试题（50）分析**

本题考查 SNMP 协议体系结构。

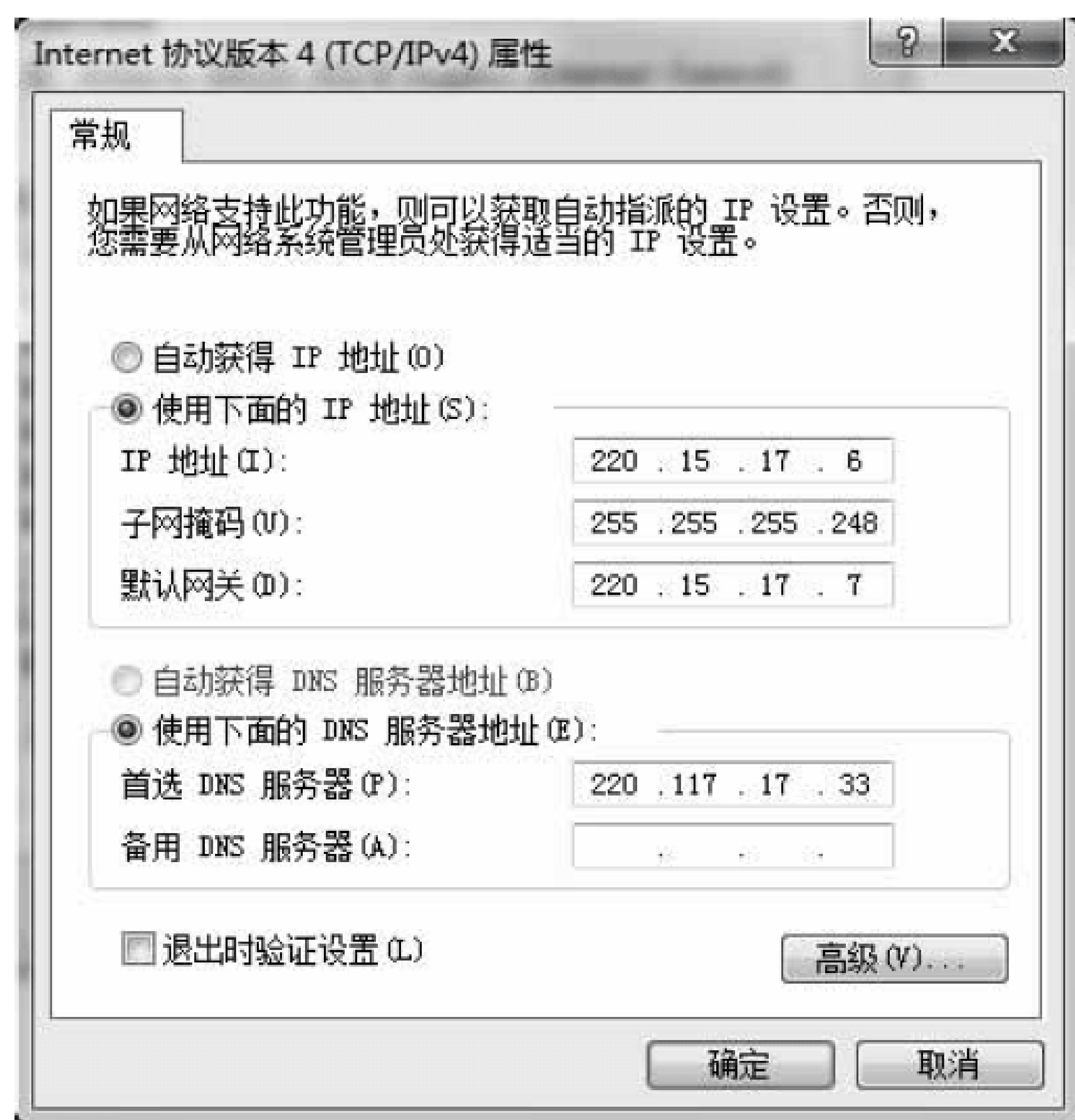
SNMP 定义为应用层协议，它依赖于 UDP 数据报服务。SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。

**参考答案**

（50）B

**试题（51）**

一台电脑的本地连接设置如下图所示，结果发现不能 ping 通任何远程设备，该故障的原因是什么？__（51）__。




（51）A．默认网关的地址不属于主机所在的子网

B．该主机的地址是一个广播地址

C．默认网关的地址是该子网中的广播地址

D．该主机的地址是一个无效的组播地址

**试题（51）分析**

在这个配置中，子网掩码是 255.255.255.248，而默认网关的地址 220.15.17.7 广播地址，这种配置是无效的。

**参考答案**

（51）C

**试题（52）**

如果指定子网掩码为 255.255.254.0，则地址__（52）__可以被赋予一个主机。

（52）A．112.10.4.0　　　　B．186.55.3.0
　　　C．117.30.3.255　　　D．17.34.36.0

**试题（52）分析**

如果指定子网掩码为 255.255.254.0，则 IP 地址的最后 9 位为主机地址，所以这 9 位不能为全 0 或全 1，由于

地址 112.10.4.0 的二进制形式是：　01110000.00001010.00000100.00000000

地址 186.55.3.0 的二进制形式是：　10111010.00110111.0000001 1.00000000

地址 117.30.3.255 的二进制形式是：　01110101.00011110.0000001 1.11111111

地址 17.34.36.0 的二进制形式是：　00010001.00100010.00100100.00000000

所以只有地址 B 可以被赋予一个主机。

**参考答案**

（52）B

**试题（53）**

某个网络中包含 320 台主机，采用什么子网掩码可以把这些主机置于同一个子网中而且不浪费地址？ （53） 。

（53）A．255.255.255.0　　　　B．255.255.254.0
　　　C．255.255.252.0　　　　D．255.255.248.0

**试题（53）分析**

320 台主机要至少要占用 9 位子网掩码，所以只有 B 是正确答案。

**参考答案**

（53）B

**试题（54）**

如果 DHCP 服务器分配的默认网关地址是 192.168.5.33/28，则主机的有效地址应该是 （54） 。

（54）A．192.168.5.55　　　　B．192.168.5.47
　　　C．192.168.5.40　　　　D．192.168.5.32

**试题（54）分析**

网关地址 192.168.5.33/28 的二进制形式是：11000000.10101000.00000101.00100001

A 地址 192.168.5.55 的二进制形式是：

11000000.10101000.00000101.00110111

B 地址 192.168.5.47 的二进制形式是：

11000000.10101000.00000101.00101111

C 地址 192.168.5.40 的二进制形式是：

11000000.10101000.00000101.00101000

D 地址 192.168.5.32 的二进制形式是：

11000000.10101000.00000101.00100000

可见答案 C 与网关地址属于同一个子网。答案 B 是同一子网中的广播地址，答案 D 是同一子网的网络地址。

**参考答案**

（54）C

**试题（55）**

4 条路由：124.23.129.0/24、124.23.130.0/24、124.23.132.0/24 和 124.23.133.0/24 经过汇聚后得到的网络地址是__（55）__。

（55）A．124.23.128.0/21　　B．124.23.128.0/22
　　　C．124.23.130.0/22　　D．124.23.132.0/23

**试题（55）分析**

地址 124.23.129.0/24 的二进制展开形式为：01111100.00010111.10000001.00000000
地址 124.23.130.0/24 的二进制展开形式为：01111100.00010111.10000010.00000000
地址 124.23.132.0/24 的二进制展开形式为：01111100.00010111.10000100.00000000
地址 124.23.133.0/24 的二进制展开形式为：01111100.00010111.10000101.00000000

所以提供 21 位子网掩码的地址 124.23.128.0/21 可以作为汇聚后的网络地址。

**参考答案**

（55）A

**试题（56）**

下面哪一个 IP 地址属于 CIDR 地址块 120.64.4.0/22?__（56）__。

（56）A．120.64.8.32　　B．120.64.7.64
　　　C．120.64.12.128　　D．120.64.3.255

**试题（56）分析**

地址块 120.64.4.0/22 的二进制形式为：　01111000.01000000.00000100.00000000
A 地址 120.64.8.32 的二进制形式为：　01111000.01000000.00001000.00100000
B 地址 120.64.7.64 的二进制形式为：　01111000.01000000.00000111.01000000
C 地址 120.64.12.128 的二进制形式为：　01111000.01000000.00001100.10000000
D 地址 120.64.3.255 的二进制形式为：　01111000.01000000.00000011.11111111

所以只有 B 答案是正确的。

**参考答案**

（56）B

**试题（57）**

两个主机通过电缆直接相连，主机 A 的 IP 地址为 220.17.33.24/28，而主机 B 的 IP 地址为 220.17.33.100/28，两个主机互相 Ping 不通，这时应该__（57）__。

（57）A．改变主机 A 的地址为 220.17.33.15

B．改变主机 B 的地址为 220.17.33.111

C．改变子网掩码为/26

D．改变子网掩码为/25

**试题（57）分析**

主机 A 地址 220.17.33.24/28 的二进制形式是：11011100.00010001.00100001.00011000

主机 B 地址 220.17.33.100/28 的二进制形式是：11011100.00010001. 00100001. 01100100

可见两个主机地址被子网掩码覆盖的部分不同，不在一个子网中，所以互相 Ping 不通。纠正的方法是缩短子网掩码到 25 位，使两个地址处于同一子网中。

**参考答案**

（57）D

**试题（58）**

下面哪个地址可以应用于公共互联网中？__（58）__。

（58）A．10.172.12.56　　B．172.64.12.23

C．192.168.22.78　　D．172.16.33.124

**试题（58）分析**

公共互联网中的地址不能是规定的私网地址，地址 10.172.12.56 是 A 类私网地址，地址 192.168.22.78 是 C 类私网地址，地址 172.16.33.124 是 B 类私网地址，都不能应用于互联网中。

**参考答案**

（58）B

**试题（59）**

下面关于 IPv6 单播地址的描述中，正确的是__（59）__。

（59）A．全球单播地址的格式前缀为 2000::/3

B．链路本地地址的格式前缀为 FE00::/12

C．站点本地地址的格式前缀为 FE00::/10

D．任何端口只能拥有唯一的全局地址

**试题（59）分析**

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，可表示为“IPv6 地址/前缀长度”的形式。IPv6 地址的具体类型是由格式前缀来区分的，这些前缀的初始分配如下表所示。

**表　IPv6 地址的初始分配**

| 分　配 | 前缀（二进制） | 占地址空间的比例 |
|---|---|---|
| 保留 | 0000 0000 | 1/256 |
| 未分配 | 0000 000 | 11/256 |
| 可聚合全球单播地址 | 001 | 1/8 |
| 链路本地单播地址 | 1111 1110 10 | 1/1024 |
| 站点本地单播地址 | 1111 1110 11 | 1/1024 |
| 组播地址 | 1111 1111 | 1/256 |

IPv6 单播地址包括可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

① 可聚合全球单播地址：在全球范围内有效，相当于 IPv4 公用地址。全球地址的设计有助于构架一个基于层次的路由基础设施。

② 本地单播地址：这种地址的有效范围仅限于本地，又分为两类：

- 链路本地地址：其格式前缀为 1111 1110 10，用于同一链路的相邻结点间的通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址（APIPA），可用于邻居发现，并且总是自动配置的，包含链路本地地址的分组不会被路由器转发。
- 站点本地地址：其格式前缀为 1111 1110 11，相当于 IPv4 中的私网地址。如果企业内部网没有连接到 Internet 上， 则可以使用这种地址。站点本地地址不能被其他站点访问，包含这种地址的分组也不会被路由器转发到站点之外。

**参考答案**

（59）A

**试题（60）**

在 Wi-Fi 安全协议中，WPA 与 WEP 相比，采用了＿（60）＿。

（60）A. 较短的初始化向量　　B. 更强的加密算法
　　C. 共享密钥认证方案　　D. 临时密钥以减少安全风险

**试题（60）分析**

有线等效保密（Wired Equivalent Privacy，WEP）是IEEE 802.11标准的一部分，其设计目的是提供与有线局域网等价的机密性。WEP 使用RC4协议进行加密，并使用CRC-32 校验保证数据的正确性。最初的 WEP 标准使用 24 比特的初始向量，加上 40比特的字符串，构成 64 比特的 WEP 密钥。后来也允许使用 104 比特的字符串，加上 24 比特的初始向量，构成 128 比特的 WEP 密钥。WEP 存在一些安全缺陷，包括初始向量（IV）雷同的可能性，以及编造的数据包等。利用 RC4 加解密原理和初始向量的特点，通过网络偷听，不要很长时间就可以把 RC4密钥破解出来。

Wi-Fi联盟为了改善 WLAN 的安全性，根据 802.11i 草案制定了WPA（Wi-Fi Protected Access）安全认证方案。WPA 的设计中包含了认证、加密和数据完整性校验三个组成部

分。首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以 128 比特的密钥和 48 位的初始向量（IV）用于RC4加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议TKIP，以更频繁地变换密钥来降低安全风险。最后，WPA 强化了数据完整性保护，使用报文完整性编码来检测伪造的数据包，并且在报文认证码中包含有帧计数器，还可以防止重放攻击。

在 IEEE 802.11i 后，Wi-Fi 联盟就按照新的安全标准对无线产品进行认证，并且把这种认证方案称为 WPA2。

**参考答案**

（60）D

**试题（61）**

生成树协议 STP 使用了哪两个参数来选举根网桥？＿（61）＿。

（61）A．网桥优先级和 IP 地址　　B．链路速率和 IP 地址
　　C．链路速率和 MAC 地址　　D．网桥优先级和 MAC 地址

**试题（61）分析**

在通过网桥互联的局域网中，每一个网桥有唯一的 MAC 地址和唯一的优先级，地址和优先级构成网桥的标识符。按照生成树算法，通常选择标识符最小的网桥作为生成树的根网桥。

**参考答案**

（61）D

**试题（62）**

关于 VLAN，下面的描述中正确的是＿（62）＿。

（62）A．一个新的交换机没有配置 VLAN
　　B．通过配置 VLAN 减少了冲突域的数量
　　C．一个 VLAN 不能跨越多个交换机
　　D．各个 VLAN 属于不同的广播域

**试题（62）分析**

虚拟局域网（Virtual Local Area Network，VLAN）是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络。虚拟局域网与物理局域网具有同样的属性，然而其中的工作站可以不属于同一物理网段。每一个 VLAN 是一个逻辑网络，发往 VLAN 之外的分组必须通过路由器进行转发。任何交换端口都可以分配给某个 VLAN，属于同一个 VLAN 的所有端口构成一个广播域，各个 VLAN 属于不同的广播域。

新交换机出厂时被预配置了 VLAN 1，交换机本身的通信（VTP 报文、CDT 组播、以及交换机发出其他报文）都发生在 VLAN 1 中。VLAN 1 被称为管理 VLAN，当然也可以用其他的 VLAN 作为管理 VLAN。为了安全起见，网络中所有交换机的默认配置都必须改变，这样，不同 VLAN 之间的访问都要经第三层设备转发，通过访问控制列表可

以过滤不必要的通信。

**参考答案**

（62）D

**试题（63）**

下面哪个协议用于承载多个 VLAN 信息？（63）。

（63）A．802.3　B．802.1q　C．802.1x　D．802.11

**试题（63）分析**

在划分成 VLAN 的交换局域网中，交换机端口之间的连接分为两种：接入链路和中继链路。接入链路只能连接具有标准以太网卡的设备，只能传送属于单个 VLAN 的数据包。中继链路则能够传送多个 VLAN 的数据包。

为了支持中继连接，应该修改原来的以太网数据包，在其中加入 VLAN 标记，以区分属于不同 VLAN 的广播域。

VLAN 帧标记有两种格式。一种是 IEEE 制定的 802.1q 协议，在原来的以太帧中增加了 4 个字节的标记（Tag）字段，如图所示，其中标记控制信息（Tag Control Information，TCI）包含 Priority、CFI 和 VID 三部分。




图　802.1q 帧格式

另一个是 Cisco 公司的交换机间链路协议（Inter-Switch Link，ISL），适用于 Cisco 的 Catalyst 系列交换机。ISL 协议在每个帧的头部增加 26 字节的帧标记，在帧尾附加 4 字节的 CRC 校验码。

**参考答案**

（63）B

**试题（64）**

以太网协议中使用物理地址的作用是什么？（64）。

（64）A．用于不同子网中的主机进行通信

B．作为第二层设备的唯一标识

C．用于区别第二层和第三层的协议数据单元

D．使得主机可以检测到未知的远程设备

**试题（64）分析**

以太网协议中的物理地址是作为第二层设备的唯一标识，通常称为 MAC 地址，每一个网卡都具有其唯一的 MAC 地址。

**参考答案**

（64）B

**试题（65）**

下面的光纤以太网标准中，支持 1000m 以上传输距离的是__（65）__。

（65）A．1000Base-FX　　B．1000Base-CX

C．1000Base-SX　　D．1000Base-LX

**试题（65）分析**

千兆以太网通常作为主干网提供无阻塞的数据传输服务。1998 年 6 月公布的 IEEE 802.3z 和 1999 年 6 月公布的 IEEE 802.3ab 已经成为千兆以太网的正式标准。它规定了四种传输介质，如下表所示。

**表　千兆以太网标准**

| 标准 | 名称 | 电缆 | 最大段长 | 特点 |
|---|---|---|---|---|
| IEEE 802.3z | 1000Base-SX | 光纤（短波 770～860nm） | 550m | 多模光纤（50，62.5μm） |
| | 1000Base-LX | 光纤（长波 1270～1355nm） | 5000m | 单模（10μm）或多模光纤（50，62.5μm） |
| | 1000Base-CX | 2 对 STP | 25m | 屏蔽双绞线，同一房间内的设备之间 |
| IEEE 802.3ab | 1000Base-T | 4 对 UTP | 100m | 5 类无屏蔽双绞线，8B/10B 编码 |

**参考答案**

（65）D

**试题（66）**

IEEE 802.11 采用了 CSMA/CA 协议，采用这个协议的原因是__（66）__。

（66）A．这个协议比 CSMA/CD 更安全

B．这种协议可以引进更多业务

C．这种协议可以解决隐蔽终端问题

D．这个协议比其他协议更有效率

**试题（66）分析**

802.11 MAC 子层的功能是提供访问控制机制，定义了 3 种访问控制机制：CSMA/CA 支持竞争访问，RTS/CTS 和点协调功能支持无竞争的访问。

CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫作载波监听多路访问/冲突避免协议。在无线网中进行冲突检测是有困难的，例如两个站由于距离过大或

者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。

**参考答案**

（66）C

**试题（67）**

配置路由器默认路由的命令是＿（67）＿。

（67）A．ip route 220.117.15.0 255.255.255.0 0.0.0.0

B．ip route 220.117.15.0 255.255.255.0 220.117.15.1

C．ip route 0.0.0.0 255.255.255.0 220.117.15.1

D．ip route 0.0.0.0 0.0.0.0 220.117.15.1

**试题（67）分析**

默认路由（Default Route）是在路由器无法找到通往目标的路径时使用的转发通路。一般来说，当路由器收到了一个分组，其目标地址在路由表中找不到时，该分组就被丢弃。这与交换机对未知分组进行泛洪（flooding）发送是不同的。在路由表中设置的默认路由是用来转发未知分组的通路。配置默认路由可以把以上命令中的目标网络号和子网掩码表示为“0.0.0.0 0.0.0.0”，其含义是“所有网络的所有主机”。

**参考答案**

（67）D

**试题（68）**

路由表如下图所示，如果一个分组的目标地址是 220.117.5.65，则会被发送给哪个端口？＿（68）＿。

| Network | interface | next-hop |
|---|---|---|
| 220.117.1.0/24 | e0 | directly connected |
| 220.117.2.0/24 | e0 | directly connected |
| 220.117.3.0/25 | s0 | directly connected |
| 220.117.4.0/24 | s1 | directly connected |
| 220.117.5.0/24 | e0 | 220.117.1.2 |
| 220.117.5.64/28 | e1 | 220.117.2.2 |
| 220.117.5.64/29 | s0 | 220.117.3.3 |
| 220.117.5.64/27 | s1 | 220.117.4.4 |

（68）A．220.117.1.2　　B．220.117.2.2

C．220.117.3.3　　D．220.117.4.4

**试题（68）分析**

如果一个分组的目标地址是 220.117.5.65，按照最长匹配原则，与之匹配的是 220.117.5.64/29，所以该分组会被发送给端口 220.117.3.3。

**参考答案**

（68）C

**试题（69）**

一家连锁店需要设计一种编址方案来支持全国各个门店销售网络，门店有300家左右，每个门店一个子网，每个子网中的终端最多50台，该连锁店从ISP处得到一个B类地址，应该采用的子网掩码是__（69）__。

（69）A．255.255.255.128　　B．255.255.252.0

C．255.255.248.0　　D．255.255.255.224

**试题（69）分析**

每个子网有50台终端，至少要占用6位地址码。300家门店需要占用9位地址码。对于B类网络，用第三字节的8位和第四字节的1位来区分不同的门店子网，用第四字节的7位作为子网内的主机地址，是一种合适的编址方案。

**参考答案**

（69）A

**试题（70）**

网络系统设计过程中，物理网络设计阶段的任务是__（70）__。

（70）A．依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B．分析现有网络和新网络的各类资源分布，掌握网络所处的状态

C．根据需求规范和通信规范，实施资源分配和安全规划

D．理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

**试题（70）分析**

物理网络是逻辑网络的具体实现，通过对设备的物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。

**参考答案**

（70）A

**试题（71）～（75）**

Traditional IP packet forwarding analyzes the __（71）__ IP address contained in the network layer header of each packet as the packet travels from its source to its final destination. A router analyzes the destination IP address independently at each hop in the network. Dynamic __（72）__ protocols or static configuration builds the database needed to analyze the destination IP address (the routing table). The process of implementing traditional IP routing also is called hop-by-hop destination-based __（73）__ routing. Although successful, and obviously widely deployed, certain restrictions, which have been realized for some time, exist for this method of packet forwarding that diminish its __（74）__. New techniques are therefore

required to address and expand the functionality of an IP-based network infrastructure. This first chapter concentrates on identifying these restrictions and presents a new architecture, known as multiprotocol （75） switching, that provides solutions to some of these restrictions.

（71）A. datagram　B. destination　C. connection　D. service
（72）A. routing　B. forwarding　C. transmission　D. management
（73）A. anycast　B. multicast　C. broadcast　D. unicast
（74）A. reliability　B. flexibility　C. stability　D. capability
（75）A. cost　B. cast　C. mark　D. label

**参考译文**

传统的 IP 分组转发机制是在分组从源端到达最终目标的旅行过程中，分析包含在每个分组网络层头部的目标 IP 地址字段。在网络的每一跳步中，路由器独立地分析目标 IP 地址字段。动态路由协议或者静态配置都建立了用于分析目标 IP 地址字段的数据库（路由表）。实现传统 IP 路由的过程也被叫作逐跳的基于目标的单播路由。虽然这种分组转发技术已经取得了成功并被广泛地部署在网络中，然而人们早已认识到，还存在一些约束条件降低了它的灵活性。因而需要一种新技术来改进和扩展基于 IP 的网络架构功能。这一章集中于识别这些约束条件，并提出一种新的体系结构，这就是多协议标记交换技术，它提供了克服这些约束条件的解决方案。

**参考答案**

（71）B　（72）A　（73）D　（74）B　（75）D

# 第 18 章　2013 上半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某学校计划部署园区网络，本部与分校区地理分布如图 1-1 所示。

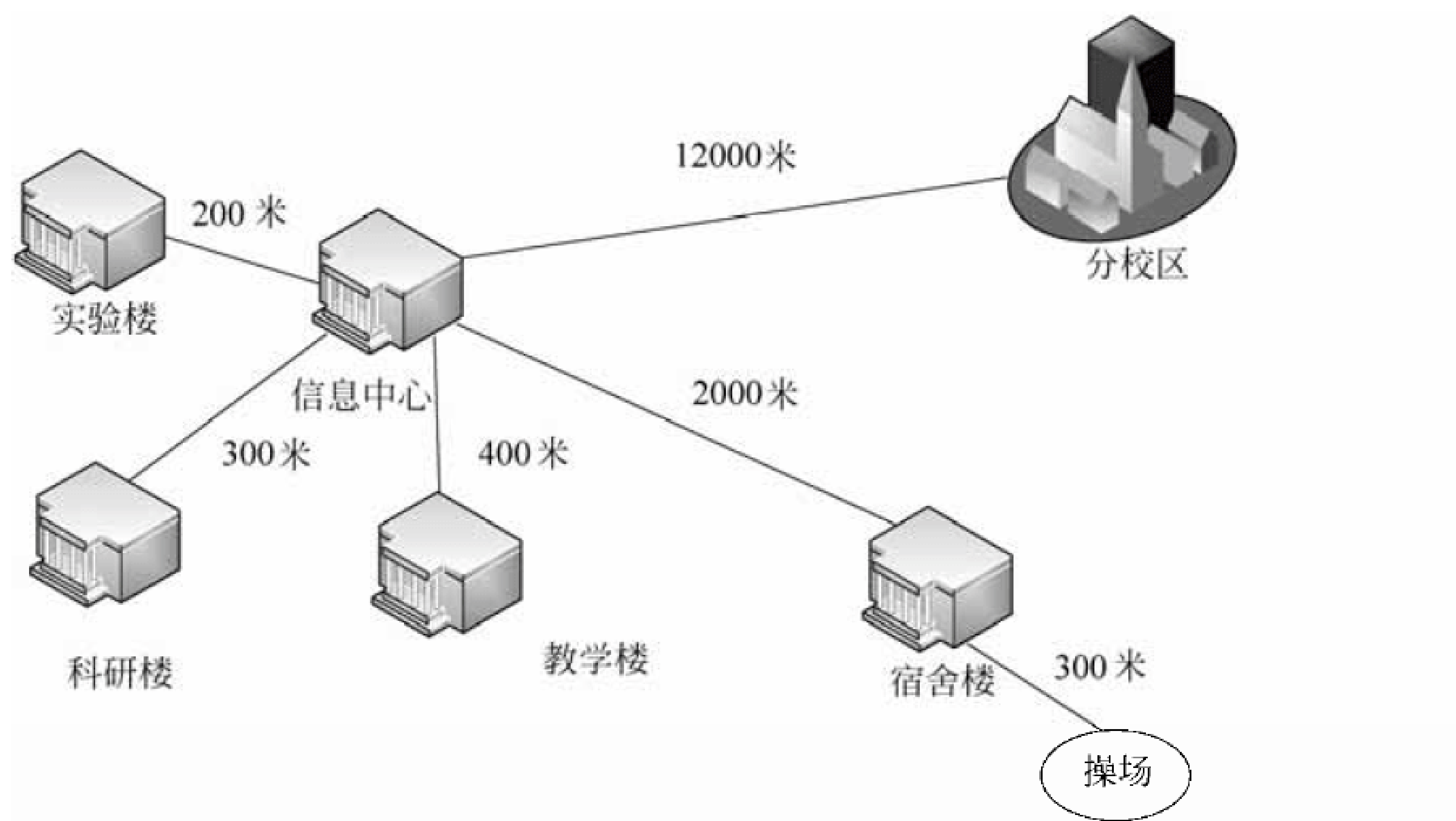



图 1-1

根据需求分析结果，网络规划部分要求如下：

1. 网络中心机房在信息中心。
2. 要求汇聚交换机到核心交换机以千兆链路聚合。
3. 核心交换机要求电源、引擎双冗余。
4. 信息中心与分校区实现互通。

**【问题 1】（4 分，每空 1 分）**

网络分析与设计过程一般采用五个阶段：需求分析、通信规范分析、逻辑网络设计、物理网络设计与网络实施。其中，确定新网络所需的通信量和通信模式属于__（1）__阶段；确定 IP 地址分配方案属于__（2）__阶段；明确网络物理结构和布线方案属于__（3）__阶段；确定网络投资规模属于__（4）__阶段。

**【问题 2】（9 分，每空 1 分）**

根据需求分析，规划该网络拓扑如图 1-2 所示。

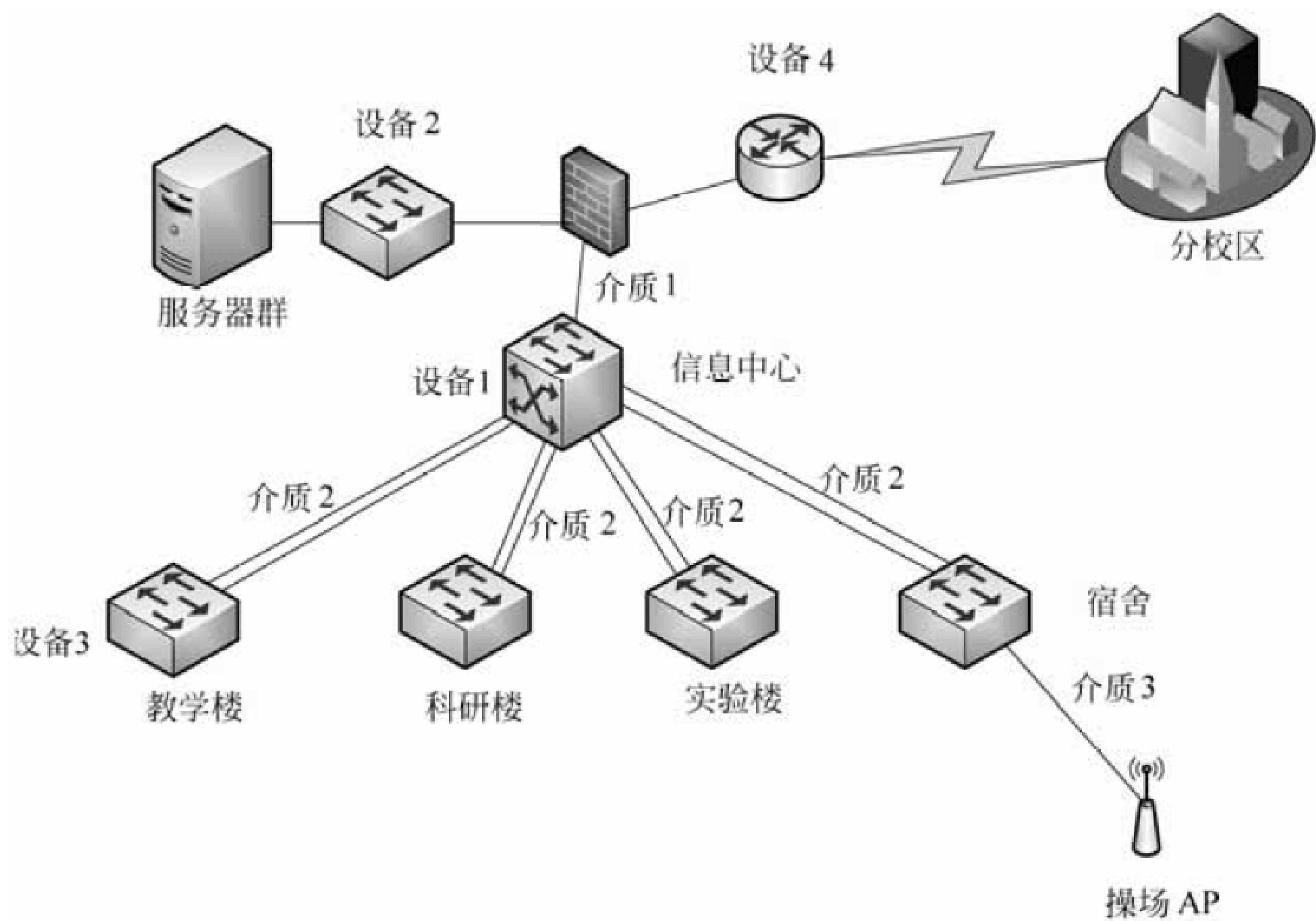



图 1-2

1．核心交换机配置如表 1-1 所示，确定核心交换机所需配备的模块最低数量。

**表 1-1**

| 设备大类 | 模块描述 | 数量 |
|---|---|---|
| 核心交换机 | 以太网交换机主机 | 1 |
| | 交换路由引擎 | (5) |
| | 交流电源模块，1400W | (6) |
| | 24 端口千兆以太网电接口板（RJ45） | 1 |
| | 12 端口千兆以太网光接口模块（SFP，LC） | (7) |
| | SFP-GE　（1310nm,LC） | (8) |

2．根据网络需求描述、网络拓扑结构、核心交换机设备表，图 1-2 中的介质 1 应选用__（9）__；介质 2 应选用__（10）__；介质 3 应选用__（11）__。

（9）～（11）备选答案：（注：每项只能选择一次）

A．单模光纤　　B．多模光纤　　C．6 类双绞线　　D．同轴电缆

3．为了网络的安全运行，该网络部署了 IDS 设备。在图 1-2 中的设备 1、2、3、4 上，适合部署 IDS 设备的是__（12）__及__（13）__。

**【问题 3】（4 分　每空 1 分）**

该校园根据需要部署了两处无线网络。一处位于学校操场，一处位于科研楼。其中操场的无线 AP 只进行用户认证，科研楼的无线 AP 中允许指定的终端接入。

（1）无线 AP 分为 FIT AP 和 FAT AP 两种。为了便于集中管理，学校的无线网络采用了无线网络控制器，所以该学校的无线 AP 为__（14）__AP。天线通常分为全向天线和定向天线，为保证操场的无线覆盖范围，此时应配备__（15）__天线。

（2）为了保证科研楼的无线 AP 的安全性，根据需求描述，一方面需要进行用户认证，另一方面还需要多接入终端的__（16）__地址进行过滤，同时为保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和 WPA2 三种方式。目前，安全性最好的是__（17）__。

**【问题 4】（3 分 ，每空 1 分）**

学校计划采用 VPN 方式实现分校区与本部的互通。VPN 的隧道协议主要有三种：PPTP，L2TP 和 IPSec，其中__（18）__和__（19）__协议工作在 OSI 模型的第二层，又称为二层隧道协议；__（20）__是第三层隧道协议。

**试题一分析**

本题考查网络规划知识与应用。

**【问题 1】**

本问题考查网络规划周期的基本知识。

网络规划一般采用五阶段周期，将网络建设划分为需求分析、通信规范分析、逻辑网络设计、物理网络设计、实施五个阶段。其中，需求分析应完成业务需求、用户需求、应用需求、计算机平台需求、网络通信需求等各项分析，其中网络投资规模属于需求分析要完成的工作。

现有的网络体系分析，即通信规范分析应完成现有网络的拓扑结构分析、容量分析，以及新网络所需的通信量和通信模式等分析。

逻辑网络设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。其中，IP 地址分配方案就属于这一阶段的工作。

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。

实施阶段就是根据以上的工作完成网络的安装和维护。

**【问题 2】**

本问题考查网络设备选型、部署及介质选择知识。

根据题目描述可知，核心交换机要求电源、引擎双冗余，而且要求汇聚交换机到核心交换机以千兆链路聚合。所以核心交换机的交换路由引擎及交流电源模块最低数量为 2 个。根据拓扑结构图，核心交换机下共有 4 个汇聚交换机，而汇聚交换机到核心交换机以千兆链路聚合，所以光模块-SFP-GE-单模模块最少需要 8 个，12 端口千兆/百兆以太网光接口模块最少需要 1 个。

根据网络需求描述、网络拓扑结构、核心交换机设备表，由于备选答案每项只能选择一次，故先判断介质 2 必须选择单模光纤，介质 3 只能选择多模光纤，所以介质 1 只能选择 6 类双绞线。

入侵检测系统是一个监听设备，无须跨接在任何链路上，不产生任何网络流量便可

以工作。因此，部署 IDS 的唯一的要求是，应当挂接在所关注流量必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量，以及需要统计、监视的网络报文。目前的网络都是交换式的拓扑结构，因此一般选择在尽可能靠近攻击源，或者尽可能接近受保护资源的地方，这些位置通常是：服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上。所以，在图 2-1 中的设备 1、2、3、4 中，适合部署 IDS 设备的是 1 及 2。

**【问题 3】**

本问题考查无线网络的基础知识。

无线 AP 分为 FIT AP 和 FAT AP 两种，FAT AP 是与 FIT AP 相对来讲的，FAT AP 将 WLAN 的实体层、加密、用户认证、网路管理等功能集于一身；而 FIT AP 是一个只有射频和通信功能的 AP，功能单一，不能独立工作。FAT AP 无线网路解决方案可由 FAT AP 直接在有线网的基础上构成，所有 AP 都单独进行配置，且难于集中管理；而 FIT AP 无线网路解决方案则是由无线网路控制器和 FIT AP 在有线网的基础上构成，且 FIT AP 上“零配置”，所有配置都集中到无线网路控制器上。易于集中管理。所以该学校的无线 AP 为 FIT AP。天线通常分为全向天线和定向天线，为保证操场的无线覆盖范围，此时应配备全向天线。

根据需求描述，科研楼的无线 AP 中允许指定的终端接入，所以为了保证科研楼的无线 AP 的安全性，一方面需要进行用户认证，另一方面还需要对接入终端的 MAC 地址进行过滤，同时为保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和 WPA2 三种方式。目前，安全性最好的是 WPA2。

**【问题 4】**

本问题考查 VPN 的基础知识。

VPN 的隧道协议主要有三种：PPTP，L2TP 和 IPSec，其中 PPTP 和 L2TP 协议工作在 OSI 模型的第二层，又称为二层隧道协议；而 IPSec 是第三层隧道协议。

**参考答案**

**【问题 1】**

（1）通信规范分析　（2）逻辑网络设计　（3）物理网络设计　（4）需求分析

**【问题 2】**

（5）2　（6）2　（7）1　（8）8　（9）C　（10）A

（11）B　（12）设备 1　（13）设备 2（（12）、（13）答案可互换）

**【问题 3】**

（14）FIT（15）全向　（16）MAC（或物理）　（17）WPA2

**【问题 4】**

（18）PPTP　（19）L2TP（（18）、（19）答案可互换）　（20）IPSec

**试题二（共 15 分）**

认真阅读下列说明信息，回答问题 1 至问题 3。将答案填入答题纸对应的解答栏内。

【说明】

某公司搭建了一个小型局域网，局域网内有 200 台 PC 机，网络中配置一台 Linux 服务器作为 Internet 接入服务器，Linux 服务器 E0 网卡的 IP 地址为 192.168.1.1，E1 网卡的 IP 地址为 202.100.20.30，该网络结构如图 2-1 所示。

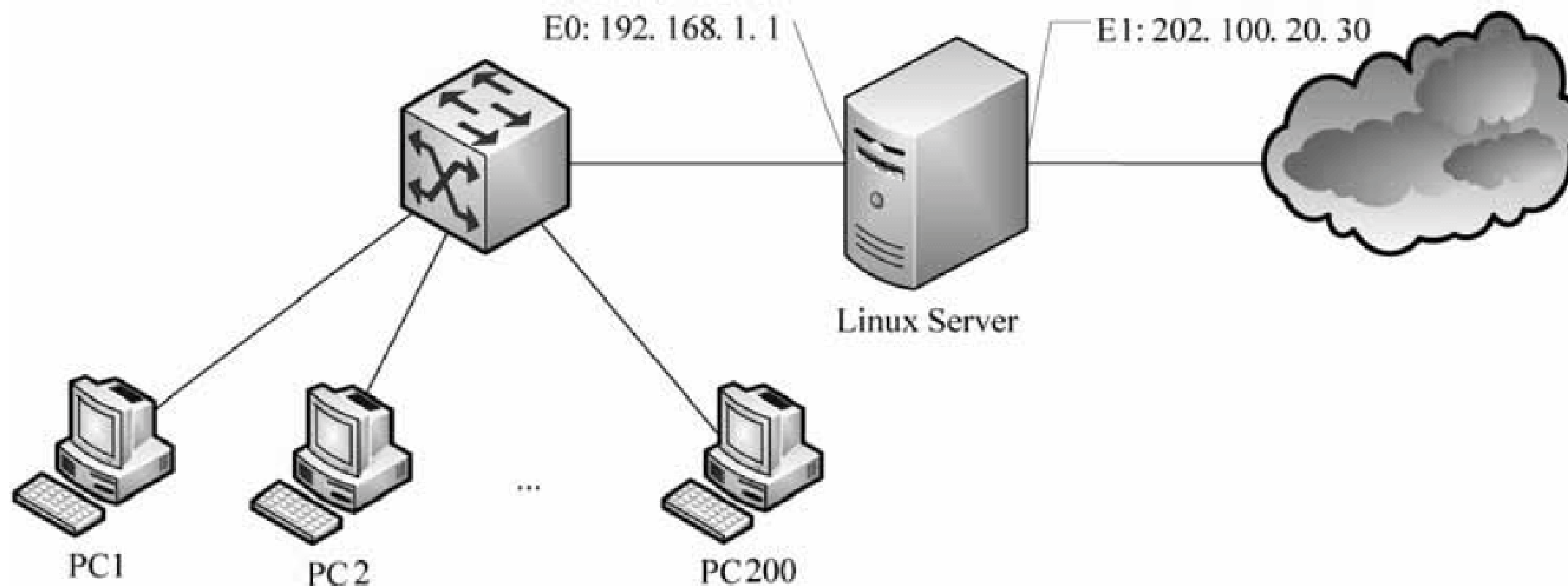



图 2-1

为了方便局域网 IP 地址管理，决定在 Linux Server 中配置 DHCP 服务，要求 DHCP 服务的配置满足几个条件：

（1）考虑今后扩展需求，当前只使用从 192.168.1.1 到 192.168.1.201 的 IP 地址；

（2）PC100（MAC 地址为 00:A0:78:8E:9E:AA）作为内部文件服务器，需要使用固定的 IP 地址 192.168.1.100；

（3）在 Linux Server 上配置 DNS 服务。

【问题 1】（9 分）

根据题目要求补充完成 DHCP 服务器配置文件 dhcpd.conf 的配置项。

```
default-lease-time 1200;
max-lease-time 9200;
option subnet-mask 255.255.255.0;
option broadcast-address __(1)__;
option routers __(2)__;
option domain-name-servers __(3)__;
subnet __(4)__ netmask __(5)__
{
range __(6) (7)__;
}
host fixed {
hardware ethernet __(8)__;
fixed-address __(9)__;
}
```

**【问题 2】（4 分）**

依据 DHCP 协议约定和问题 1 中的配置，DHCP 客户端 PC1 从获取 IP 地址后经过 （10） 分钟需要到 DHCP 服务器申请租约更新。此时 PC1 发送到 DHCP 服务器的消息是 （11） ，如果 DHCP 服务器同意租约更新，响应的消息是 （12） ，如果 DHCP 服务器不同意租约更新，响应的消息是 （13） 。

**【问题 3】（2 分）**

在 DHCP 客户端，还可以通过命令 （14） 来立即释放申请到的 IP 地址，通过命令 （15） 来立即重新申请租约。

**试题二分析**

本题主要考查考生对 Linux 系统中 DHCP 服务 dhcpd 配置等相关知识点的掌握情况。

**【问题 1】**

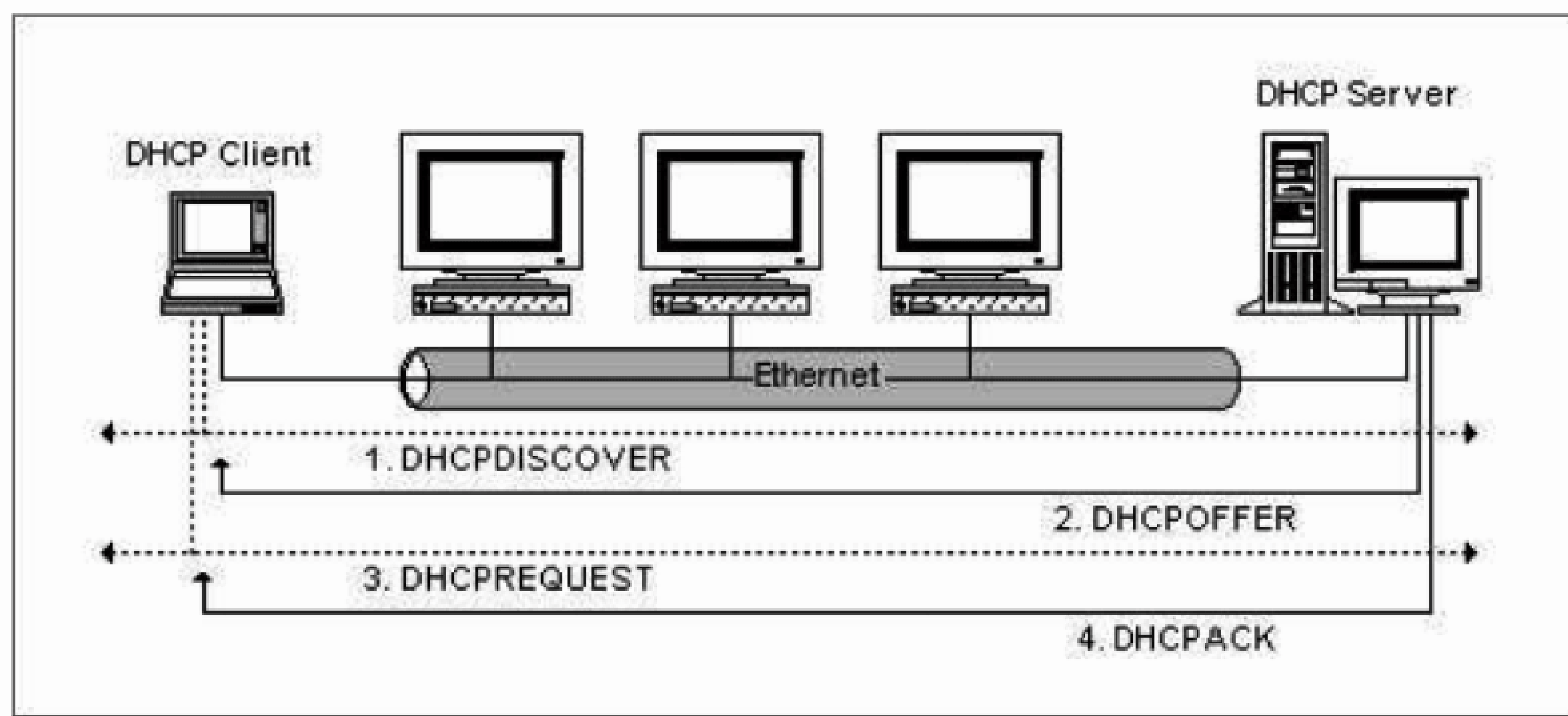
Linux 的 DHCP 服务是通过 dhcpd 提供的，该服务通过配置文件 dhcpd.conf 对服务参数等进行设置，相应的命令和解释如下：

```
default-lease-time 1200; //设置默认租期，单位为秒，DHCP 客户端请求 IP 地址时如
                         果没有带租约参数，则 DHCP 服务器为客户端设置租期为默认租期
max-lease-time 9200; //设置客户端最长租期，单位为秒，DHCP 客户端请求 IP 地址时如
                         果请求租约超过该最长租期，则 DHCP 服务器为客户端设置租期为该租期
 option subnet-mask 255.255.255.0;         //设置子网掩码
 option broadcast-address  （1） ;          //设置子网广播地址
 option routers  （2） ;                    //设置网关地址
 option domain-name-servers  （3） ;        //设置 DNS 服务器地址
 subnet  netmask                           //设置一个子网
 range                                 //起始 IP 终止 IP 提供动态分配 IP 的范围
 host                                      //参考特别的主机
 hardware ethernet                         //指定 MAC 地址
 fixed-address                             //保留的 IP 地址
```

**【问题 2】**

依据 DHCP 协议约定，DHCP 客户端从获取 IP 地址后到租约时间的 50%需要到 DHCP 服务器申请租约更新，从问题 1 中的配置可以得出默认租约是 1200 秒（20 分钟），所以 DHCP 客户端 PC1 从获取 IP 地址后经过 10 分钟需要到 DHCP 服务器申请租约更新。

DHCP 客户端和服务器交互的消息序列如下图所示。




从图中可知，此时 PC1 发送到 DHCP 服务器的消息是 DHCPREQUEST，如果 DHCP 服务器同意租约更新，响应的消息是 DHCPACK，如果 DHCP 服务器不同意租约更新，响应的消息是 DHCPNAK。

**【问题 3】**

在 DHCP 客户端，ifconfig 可以用于网络接口配置相关操作，带上参数也可以用于发送 DHCP 协议消息，可以通过命令 ipconfig/release 来立即释放申请到的 IP 地址，通过命令 ipconfig/renew 来立即重新申请租约。

**参考答案**

**【问题 1】**

（1）192.168.1.255 （2）192.168.1.1 （3）192.168.1.1 （4）192.168.1.0

（5）255.255.255.0 （6）192.168.1.2 （7）192.168.1.201

（8）00:A0:78:8E:9E:AA （9）192.168.1.100

**【问题 2】**

（10）10 （11）DHCPREQUEST

（12）DHCPACK （13）DHCPNAK

**【问题 3】**

（14）ipconfig/release

（15）ipconfig/renew

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某学校的图书馆电子阅览室已经连接为局域网（局域网段 192.168.1.0/24），在原有接入校园网的基础上又租用了一条电信的 ADSL 宽带接入来满足用户的上网需求。其中，校园网网段为 210.27.176.0～210.27.191.255，DNS 为 210.27.176.3，子网按照 C 类网络划

分，每个子网的网关都为 210.27.xxx.1。具体网络结构如图 3-1 所示。

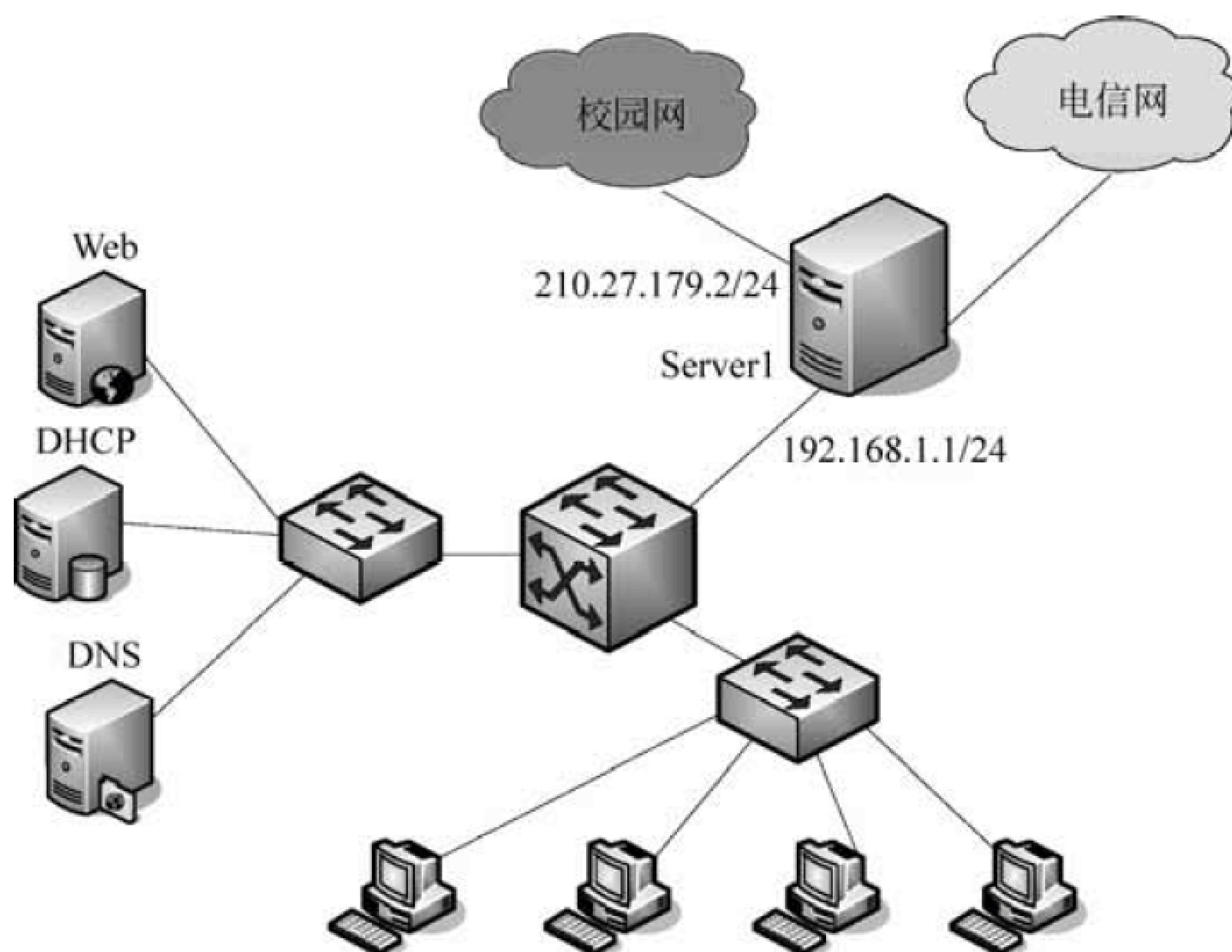



图 3-1

**【问题 1】（6 分）**

如图 3-1 所示，在该电子阅览室网络的出口利用了一台安装 Windows Server 2003 的服务器实现客户机既能访问本校和本馆内的电子资源，又能够通过 ADSL 访问外部资源。现计划在 Server1 上安装 3 块网卡来实现这个功能，三块网卡首先需要在如图 3-2 所示的界面里配置 IP 地址等信息。按照题目要求选择（1）～（6）中的正确选项。

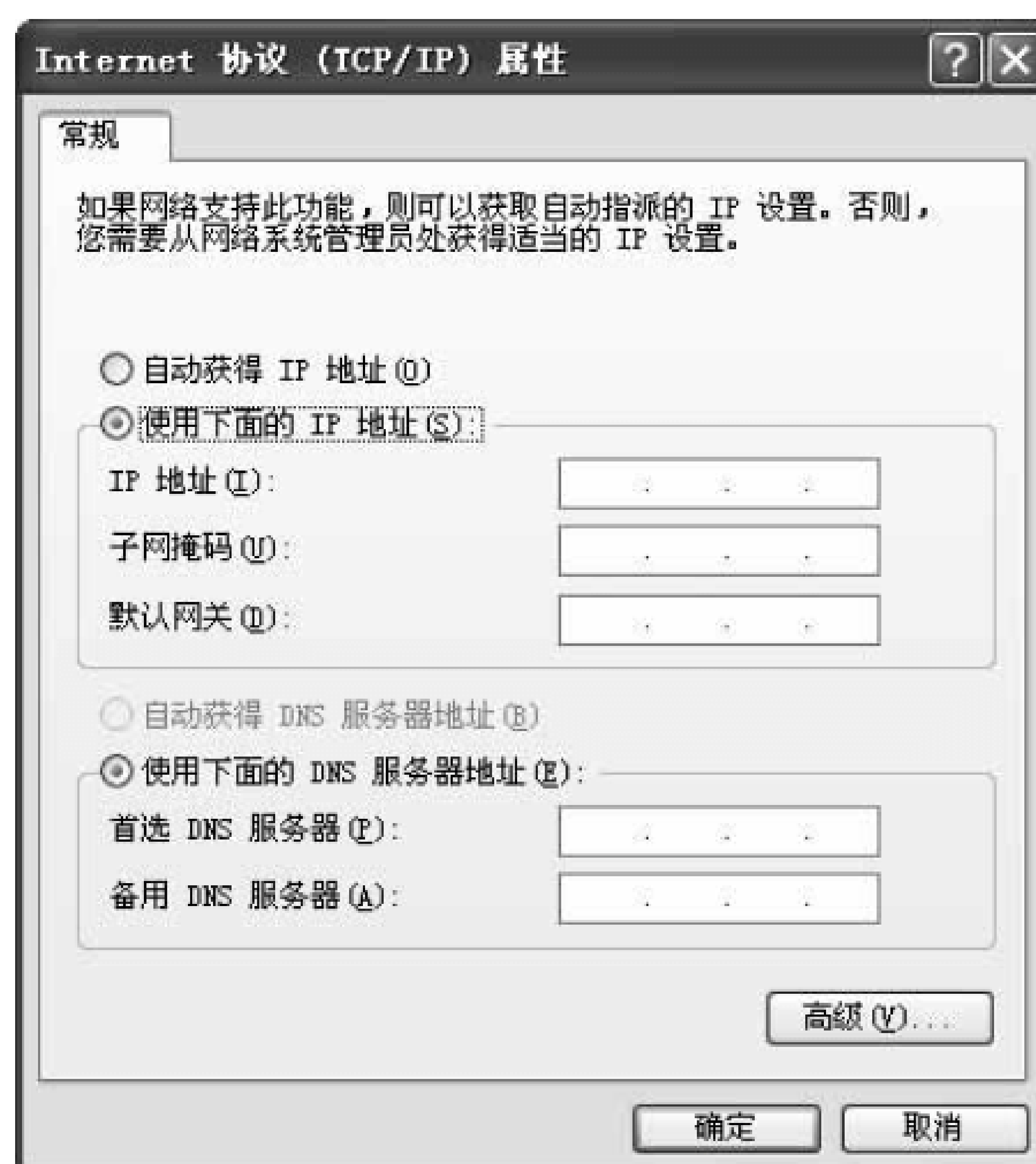



图 3-2

网卡 1：连接电子阅览室内网，IP 地址：192.168.1.1，子网掩码：255.255.255.0。

网关：__(1)__，DNS：__(2)__。

网卡 2：连接 ADSL 电信网，IP 地址：__(3)__，DNS：__(4)__。

网卡 3：连接校园网，IP 地址：__(5)__，子网掩码：255.255.255.0。

网关：__(6)__，DNS：210.27.176.3。

（1）～（6）备选答案：

A．192.168.1.1　　B．自动获取　　C．192.168.1.2

D．不指定，保持为空　　E．210.27.179.2　　F．210.27.179.1

G．255.255.255.0

**【问题 2】（8 分）**

在 Server1 上开启路由和远程访问服务，出现如图 3-3 所示的窗口，在继续配置“网络接口”时，出现如图 3-4 所示的对话框，应该选择 “__(7)__”，然后输入 ADSL 账号和密码完成连接建立过程。




图 3-3

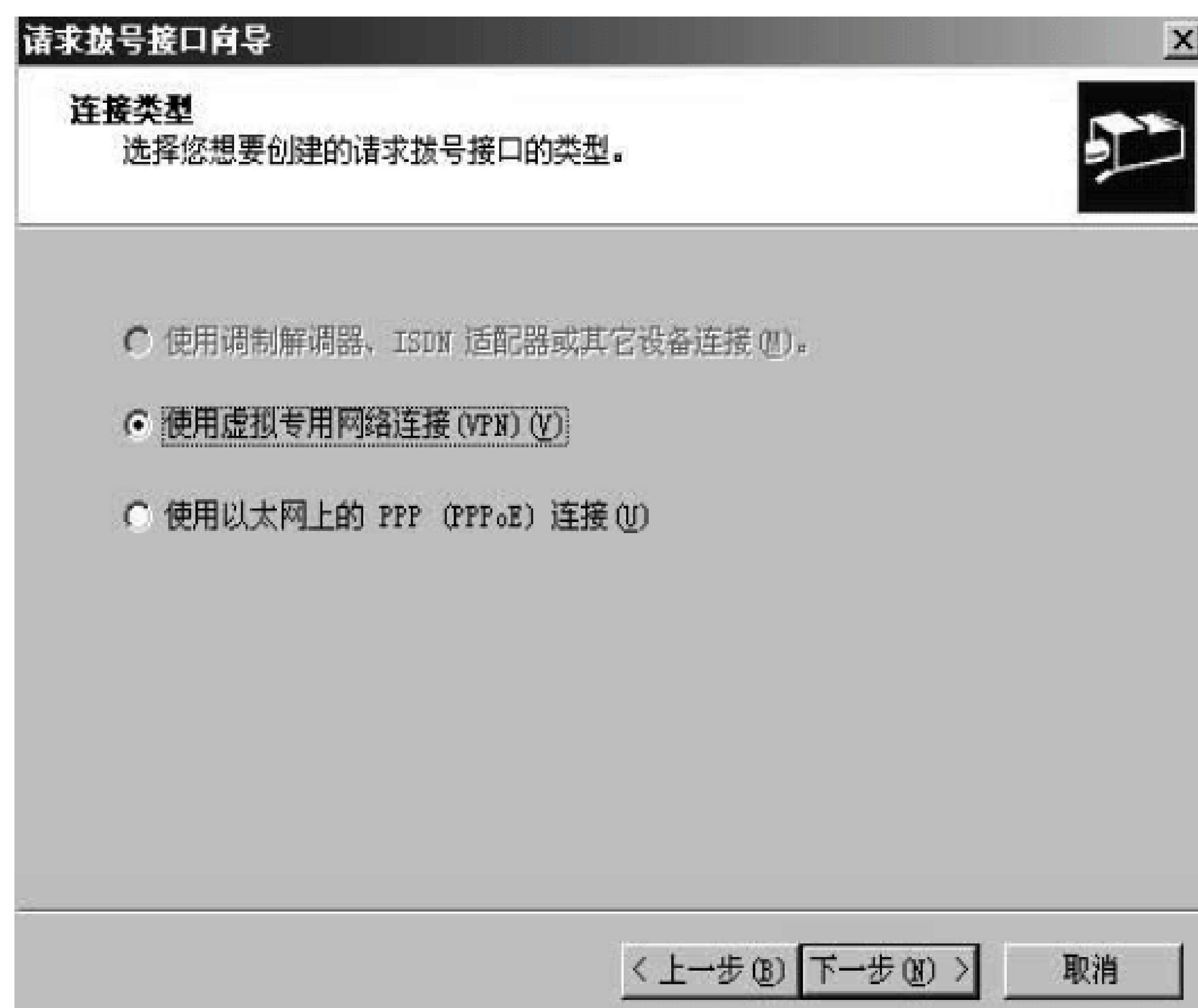



图 3-4

为了使客户机自动区分电子阅览室内网、校园网和 ADSL 电信网，还需新建一个批处理文件 route.bat，并把路由功能加入到服务器中，route.bat 文件内容如下所示，完成相关配置。

```
cd\
route delete ____(8)____ //删除默认路由
route add ____(9)____ mask 255.255.255.0 192.168.1.1 //定义内网路由
route add ____(10)____ mask 255.255.255.0 210.27.179.1
//定义校园网一个网段路由
… … //依次定义校园网其他各网段路由
```

**【问题 3】（2 分）**

因为电子阅览室的 DHCP 服务器设备老化需要更换，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这时采用导入导出方式进行配置的迁移，采用的步骤如下：

（1）在原有的 DHCP 服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt” 命令，将该文件复制到新服务器的相同位置。

（2）在新的服务器上安装好 DHCP 服务后，在命令行模式下输入“____（11）____”命令，即可完成 DHCP 服务器的迁移。

（3）在迁移操作时，一定要使用系统____（12）____组的有效账户。

**【问题 4】（4 分）**

（1）若电子阅览室的客户机访问 Web 服务器时，出现“HTTP 错误 401.1 - 未经授权：访问由于凭据无效被拒绝。”现象，则需要在控制面板→管理工具→计算机管理→本地用户和组，将____（13）____账号启用来解决此问题。

（2）若出现“HTTP 错误 401.2 -未经授权：访问由于服务器配置被拒绝。”的现象，造成错误的原因是身份验证设置的问题，一般应将其设置为____（14）____身份认证。

（13）、（14）备选答案：

A．IUSR_机器名　　B．Administrator　　C．Guest　　D．匿名

**试题三分析**

本题考查网络地址规划、Windows Server 2003 的路由与远程服务和 DHCP 服务配置以及 Web 服务故障排查方面的知识。

**【问题 1】**

本问题考查网络地址规划方面的知识。根据电子阅览室的网络拓扑图以及题目给出的提示，连接电子阅览室内网的网段为 192.168.1.0/24，只有一个网段不需要跨网段访问，所以网关以及 DNS 皆可不用指定，保持为空即可；通过 ADSL 宽带接入到电信网的网卡一般利用 PPPoE 协议接入，接入网卡的 IP 地址和 DNS 都采用动态获取方式获得；接入到校园网的网卡地址题目中已经明确给出利用静态分配的方式，符合题目要求的 IP 地址选项只能是 210.27.179.2，而网关地址只能是 210.27.179.1。

【问题 2】

本问题考查 Windows Server 2003 的路由与远程服务相关知识。

在 Server1 上开启路由和远程访问服务，题目明确要求“新建请求拨号接口”，而根据题意拨号接口采用的是 ADSL 方式接入电信网，ADSL 接入方式一般采用的是 PPPoE 协议，因此在图 3-4 的连接类型中只能选择“使用以太网上的 PPP（PPPoE）连接”这个选项。

同时为了使客户机自动区分电子阅览室内网、校园网和 ADSL 电信网，在该题目中还需在 Server1 上新建一个批处理文件 route.bat，并把路由功能加入到服务器中，即把 Server1 当作路由器来使用，只是使用的命令是 windows 支持的配置命令。具体来说 route.bat 文件的内容解释如下：

```
cd\
route delete  0.0.0.0  //删除默认路由
route add  192.168.1.0  mask 255.255.255.0 192.168.1.1  //定义内网路由
route add  210.27.176.0  mask 255.255.255.0 210.27.179.1 //定义校园网一个
                                                          网段路由
route add  210.27.177.0  mask 255.255.255.0 210.27.179.1
… …
route add  210.27.191.0  mask 255.255.255.0 210.27.179.1
//依次定义校园网其他各网段路由
```

【问题 3】

本问题考查 Windows Server 2003 DHCP 服务器迁移的相关知识。

当需要更换 Windows Server 2003 DHCP 服务器设备时，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这时可以使用导入导出 DHCP 数据库的方式，实现 DHCP 服务器从一台服务器设备转移到另一台服务器设备上。具体操作是在原有的 DHCP 服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt” 命令，开始执行本服务器 DHCP 数据库的导出，导出目录和文件名为“c:\dhcpbackup.txt”；接着将该文件复制到新服务器的相同位置，打开新的服务器的命令行界面，输入“netsh dhcp server import c:\dhcpbackup.txt”命令，将复制的 DHCP 数据库文件导入本机中。不过要注意的是在迁移操作中，一定要使用系统管理员组的有效账户，如果新服务器要升级为域控制器，尽量先做迁移后再做域身份的升级。

【问题 4】

本问题考查 WEB 访问中的故障排查的相关知识。

（1）错误现象一：HTTP 错误 401.1 - 未经授权：访问由于凭据无效被拒绝。

原因分析：由于用户匿名访问使用的账号是 IUSR_机器名，因此如果此账号被禁用，将造成用户无法访问。

解决办法：控制面板→管理工具→计算机管理→本地用户和组，将 IUSR_机器名账

号启用。

（2）错误现象二：HTTP 错误 401.2 - 未经授权：访问由于服务器配置被拒绝。

原因分析：

IIS 支持以下几种 Web 身份验证方法：

（1）匿名身份验证。

IIS 创建 IUSR_计算机名称账户（其中计算机名称是正在运行 IIS 的服务器的名称），用来在匿名用户请求 Web 内容时对他们进行身份验证。此账户授予用户本地登录权限。你可以将匿名用户访问重置为使用任何有效的 Windows 账户。

（2）基本身份验证。

使用基本身份验证可限制对 NTFS 格式 Web 服务器上的文件的访问。使用基本身份验证，用户必须输入凭据，而且访问是基于用户 ID 的。用户 ID 和密码都以明文形式在网络间进行发送。

（3）Windows 集成身份验证。

Windows 集成身份验证比基本身份验证安全，而且在用户具有 Windows 域账户的内部网环境中能很好地发挥作用。在集成的 Windows 身份验证中，浏览器尝试使用当前用户在域登录过程中使用的凭据，如果尝试失败，就会提示该用户输入用户名和密码。如果你使用集成的 Windows 身份验证，则用户的密码将不传送到服务器。如果该用户作为域用户登录到本地计算机，则他在访问此域中的网络计算机时不必再次进行身份验证。

（4）摘要身份验证。

摘要身份验证克服了基本身份验证的许多缺点。在使用摘要身份验证时，密码不是以明文形式发送的。另外，你可以通过代理服务器使用摘要身份验证。摘要身份验证使用一种挑战/响应机制（集成 Windows 身份验证使用的机制），其中的密码是以加密形式发送的。

（5）.NET Passport 身份验证。

Microsoft .NET Passport 是一项用户身份验证服务，它允许单一签入安全性，可使用户在访问启用了 .NET Passport 的 Web 站点和服务时更加安全。启用了 .NET Passport 的站点会依靠 .NET Passport 中央服务器来对用户进行身份验证。但是，该中心服务器不会授权或拒绝特定用户访问各个启用了 .NET Passport 的站点。

解决方法：

根据需要配置不同的身份认证（一般为匿名身份认证，这是大多数站点使用的认证方法）。认证选项在 IIS 的属性→安全性→身份验证和访问控制下配置。

**参考答案**

**【问题 1】**

（1）D　（2）D　（3）B　（4）B　（5）E　（6）F

**【问题 2】**

（7）使用以太网上的 PPP（PPPoE）连接

（8）0.0.0.0　（9）192.168.1.0　（10）210.27.176.0

【问题 3】

（11）netsh dhcp server import c:\dhcpbackup.txt

（12）Administrators 或 系统管理员

【问题 4】

（13）A （14）D

**试题四（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业的网络结构如图 4-1 所示。

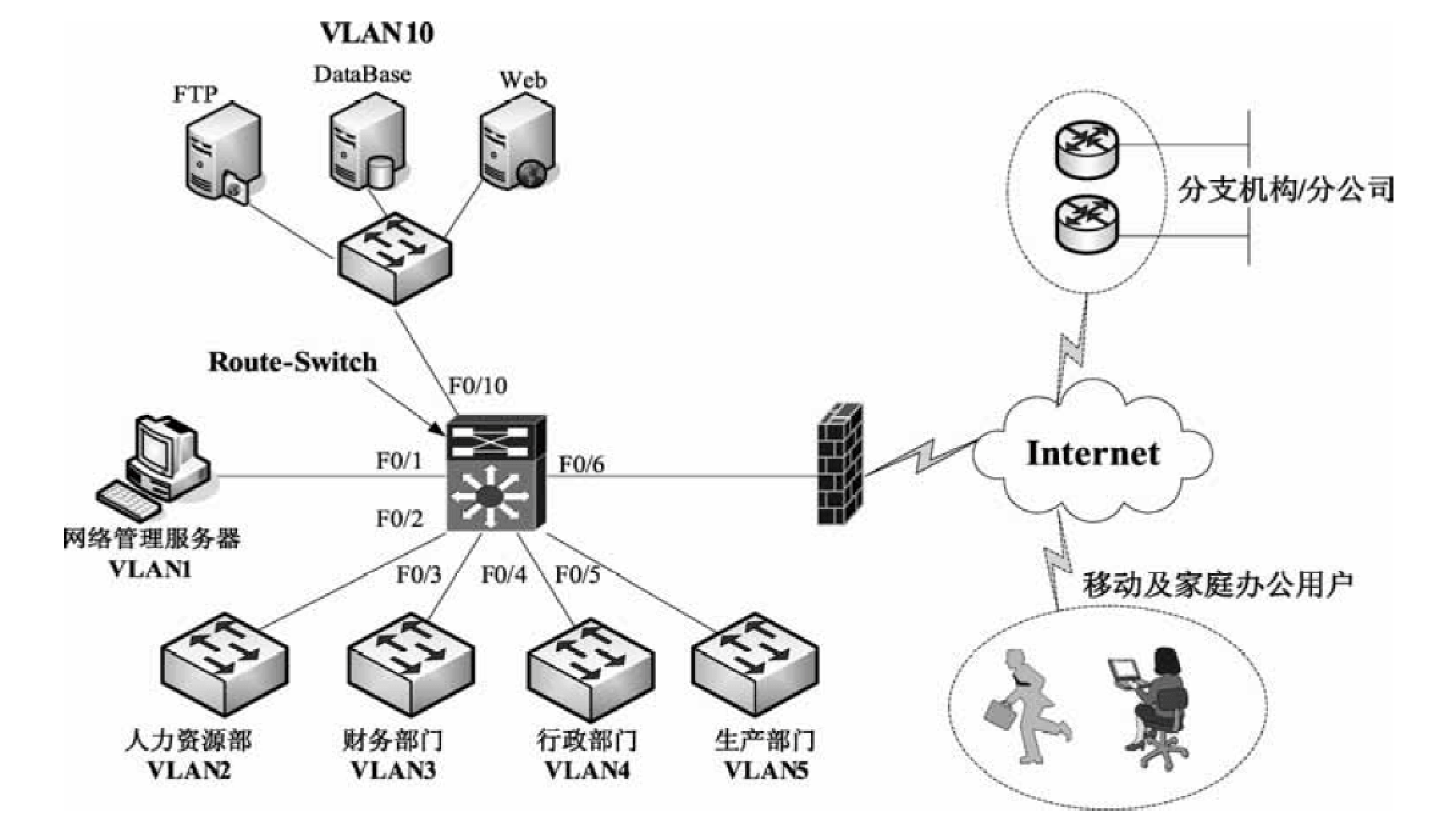



图 4-1

按照网络拓扑结构为该企业网络进行 IP 地址和 VLAN 规划，具体规划如表 4-1 所示。

**表 4-1 网络规划地址表**

| VLAN | IP 地址分配 | 服务器 | IP 地址分配 |
|---|---|---|---|
| VLAN1（管理 VLAN） | 192.168.100.0/24 | 网络管理服务器 | 192.168.100.10 |
| VLAN2（人力资源部） | 192.168.2.0/24 | FTP 服务器 | 192.168.10.10 |
| VLAN3（财务部门） | 192.168.3.0/24 | DataBase 服务器 | 192.168.10.20 |
| VLAN4（行政部门） | 192.168.4.0/24 | Web 服务器 | 192.168.10.30 |
| VLAN5（生产部门） | 192.168.5.0/24 | | |
| VLAN10（内网服务器） | 192.168.10.0/24 | | |

**【问题 1】（3 分）**

访问控制列表 ACL 可以通过编号或__(1)__来引用；ACL 分为两种类型，其中__(2)__ACL 只能根据源地址进行过滤，__(3)__ACL 使用源地址、目标地址、上层协议以及协议信息进行过滤。

**【问题 2】（6 分）**

在网络使用中，该企业要求所有部门都可以访问 FTP 和 Web 服务器，只有财务部可以访问 DataBase 服务器；同时，网络管理员可以访问所有网络资源，禁止非网络管理员访问交换设备。根据需求，完成核心交换机 Route-Switch 以下配置命令。

```
Route-Switch(config)#access-list 101 permit ip host 192.168.100.10 any
Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.10
eq ftp
Route-Switch(config)#access-list 101 ________(4)________ eq www
//允许所有主机访问 Web 服务器
Route-Switch(config)#access-list 101 ________(5)________
//允许财务部访问 DataBase 服务器
Route-Switch(config)#access-list 101 deny any any
Route-Switch(config)# int VLAN 10
Route-Switch(config-if)#ip access-group 101 in //在 VLAN10 的入方向应用 acl
101
Route-Switch(config)#access-list 102 deny any any
Route-Switch(config)# int VLAN 1
Route-Switch(config-if)#______(6)______
//禁止非网管员用户访问网络设备和网管服务器等
```

**【问题 3】（8 分）**

企业员工访问互联网时，为了财务部门的安全，必须限制财务部门的互联网访问请求；要求员工只能在周一至周五 08:00—18:00 和周末 08:00—12:00 这两个时间段访问互联网。根据需求，完成（或解释）核心交换机 Route-Switch 的部分配置命令。

```
Route-Switch(config)#time-range telnettime //定义时间范围
Route-Switch(config-time-range)#periodic weekday ___(7)___
//定制周期性执行时间为工作日的 08:00—18:00
Route-Switch(config-time-range)#periodic weekend 08:00 to 12:00
//___(8)___
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 104 deny ip 192.168.3.0 0.0.0.255 any
//___(9)___
Route-Switch(config)#access-list 104 permit ip any any time-range
telnettime
//应用访问控制时间，定义流量筛选条件
Route-Switch(config)# int f0/6
```

```
Route-Switch(config-if)#______(10)______
//在接口 F0/6 的出方向应用 acl104 规则
```

**【问题 4】（3 分）**

随着企业业务的不断扩大，企业新建了很多分支机构，为了满足各地新建分支机构和移动办公人员使用企业网络的需求，比较经济快捷的做法是选择 VPN 技术来实现这种办公需求。该技术根据连接主体的不同，针对移动办公和家庭用户可以采用的连接方式为__(11)__连接方式，针对分支机构长期性的使用可以采用__(12)__连接方式。

**试题四分析**

本题考查企业网访问控制列表和 VLAN 结合使用的相关配置知识。

**【问题 1】**

本问题考查核心访问控制列表的基本知识。

访问控制列表（ACL）是最常用的网络流量限制技术，通过该技术可以为路由器或者交换机的接口配置一些控制命令，用来控制接口的进出数据包。配置 ACL 主要有两步，首先要指定访问控制条件，需要创建列表编号或者名称；然后在指定的列表编号或者名称内添加流量筛选条件，并指定是允许还是拒绝。

访问控制列表根据筛选条件不同，一般可以分为两种标准访问控制列表和扩展访问控制列表。其中标准访问控制列表只可以限定源地址的流量，通常使用 1～99 的列表编号。而扩展访问控制列表可以针对源地址、目标地址、传输层协议、源端口、目标端口等进行流量控制，通常使用 100～199 的列表编号。

**【问题 2】**

本问题考查核心交换机 Route-Switch 扩展访问控制列表的配置知识，主要用来配置各个 VLAN 主机对内网服务器的访问权限。

```
Route-Switch(config)#access-list 101 permit ip host 192.168.100.10 any
//允许网管服务器访问内网的所有主机
Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.10 eq ftp
//允许所有主机访问 FTP 服务器 192.168.10.10 的 FTP 端口
Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.30 eq www
//允许所有主机访问 Web 服务器 192.168.10.30 的 WWW 服务端口
Route-Switch(config)#access-list 101 permit tcp 192.168.3.0 0.0.0.255 host 192.168.10.20
//允许财务部网络 192.168.3.0/24 访问 DataBase 服务器
Route-Switch(config)#access-list 101 deny any any
Route-Switch(config)# int VLAN 10
Route-Switch(config-if)#ip access-group 101 in
```

```
//在 VLAN10 的入方向应用 acl 101
Route-Switch(config)#access-list 102 deny any any
Route-Switch(config)# int VLAN 1
Route-Switch(config-if)# ip access-group 102 in
//禁止非网管员用户访问网络设备和网管服务器等
...
```

**【问题 3】**

本问题考查核心交换机 Route-Switch 定时访问控制列表的配置知识，主要用来设置互联网的访问权限。

```
Route-Switch(config)#time-range telnettime  //定义时间范围
Route-Switch(config-time-range)#periodic weekday 08:00 to 18:00
//定制周期性执行时间为工作日的 08:00—18:00
Route-Switch(config-time-range)#periodic weekend 08:00 to 12:00
//定制周期性执行时间为周末的 08:00—18:00
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 104 deny ip 192.168.3.0 0.0.0.255 any
//禁止财务部访问互联网
Route-Switch(config)#access-list 104 permit ip any any time-range telnettime
//应用访问控制时间，定义流量筛选条件
Route-Switch(config)# int f0/6
Route-Switch(config-if)# ip access-group 104 out
//在接口 F0/6 的出方向应用 acl104 规则
```

**【问题 4】**

本问题考查 VPN，即虚拟专用网的基础知识。

VPN 技术用于实现局域网络之间通过 Internet 公共网络安全地传递数据。VPN 技术根据两端的连接主体不同，可以分为远程访问的 VPN 和站点到站点的 VPN。

远程访问的 VPN 适用于建立临时性的 VPN 连接，家庭和移动办公用户使用的比较多。只需要企业网络中配置有软件或者硬件形式的 VPN 设备，家庭和移动办公用户就可以通过自己的客户端直接建立 VPN 连接请求。

站点到站点的 VPN 连接可以建立长期的 VPN 连接，适合公司总部和子公司之间长期进行数据传输。需要两端网络中都有配置好的 VPN 软件程序或硬件设备，并且有匹配的认证加密配置。

**参考答案**

**【问题 1】**

（1）名字　（2）标准　（3）扩展

【问题 2】

（4）permit tcp any host 192.168.10.30

（5）permit tcp 192.168.3.0 0.0.0.255 host 192.168.10.20

（6）ip access-group 102 in

【问题 3】

（7）08:00 to 18:00

（8）定制周期性执行时间为周末的 08:00—12:00

（9）禁止财务部访问互联网

（10）ip access-group 104 out

【问题 4】

（11）远程访问的 VPN　（12）站点到站点的 VPN

# 第 19 章　2013 下半年网络工程师上午试题分析与解答

**试题（1）**

在程序执行过程中，Cache 与主存的地址映像由__（1）__。

（1）A．硬件自动完成　　　　B．程序员调度
　　 C．操作系统管理　　　　D．程序员与操作系统协同完成

**试题（1）分析**

本题考查计算机系统基础知识。

Cache 的工作是建立在程序与数据访问的局部性原理上。经过对大量程序执行情况的结果分析：在一段较短的时间间隔内程序集中在某一较小的内存地址空间执行，这就是程序执行的局部性原理。同样，对数据的访问也存在局部性现象。

为了提高系统处理速度才将主存部分存储空间中的内容复制到工作速度更快的 Cache 中，同样为了提高速度的原因，Cache 系统都是由硬件实现的。

**参考答案**

（1）A

**试题（2）**

指令寄存器的位数取决于__（2）__。

（2）A．存储器的容量　　　　B．指令字长
　　 C．数据总线的宽度　　　D．地址总线的宽度

**试题（2）分析**

本题考查计算机系统基础知识。

指令寄存器是 CPU 中的关键寄存器，其内容为正在执行的指令，显然其位数取决于指令字长。

**参考答案**

（2）B

**试题（3）**

若计算机存储数据采用的是双符号位（00 表示正号、11 表示负号），两个符号相同的数相加时，如果运算结果的两个符号位经__（3）__运算得 1，则可断定这两个数相加的结果产生了溢出。

（3）A．逻辑与　　B．逻辑或　　C．逻辑同或　　D．逻辑异或

**试题（3）分析**

本题考查计算机系统基础知识。

当表示数据时并规定了位数后，其能表示的数值范围就确定了，在两个数进行相加运算的结果超出了该范围后，就发生了溢出。在二进制情况下，溢出时符号位将变反，即两个正数相加，结果的符号位是负数，或者两个负数相加，结果的符号位是正数。采用两个符号位时，溢出发生后两个符号位就不一致了，这两位进行异或的结果一定为 1。

**参考答案**

（3）D

**试题（4）**

若某计算机字长为 32 位，内存容量为 2GB，按字编址，则可寻址范围为__（4）__。

（4）A．1024M　　B．1GB　　C．512M　　D．2GB

**试题（4）分析**

本题考查计算机系统基础知识。

内存容量 2GB=2*1024*1024*1024*8 位，按字编址时，存储单元的个数为 2*1024*1024*1024*8/32=512*1024*1024，即可寻址范围为 512MB。

**参考答案**

（4）C

**试题（5）**

视频信息是连续的图像序列，__（5）__是构成视频信息的基本单元。

（5）A．帧　　B．场　　C．幅　　D．像素

**试题（5）分析**

本题考查多媒体方面的基础知识。

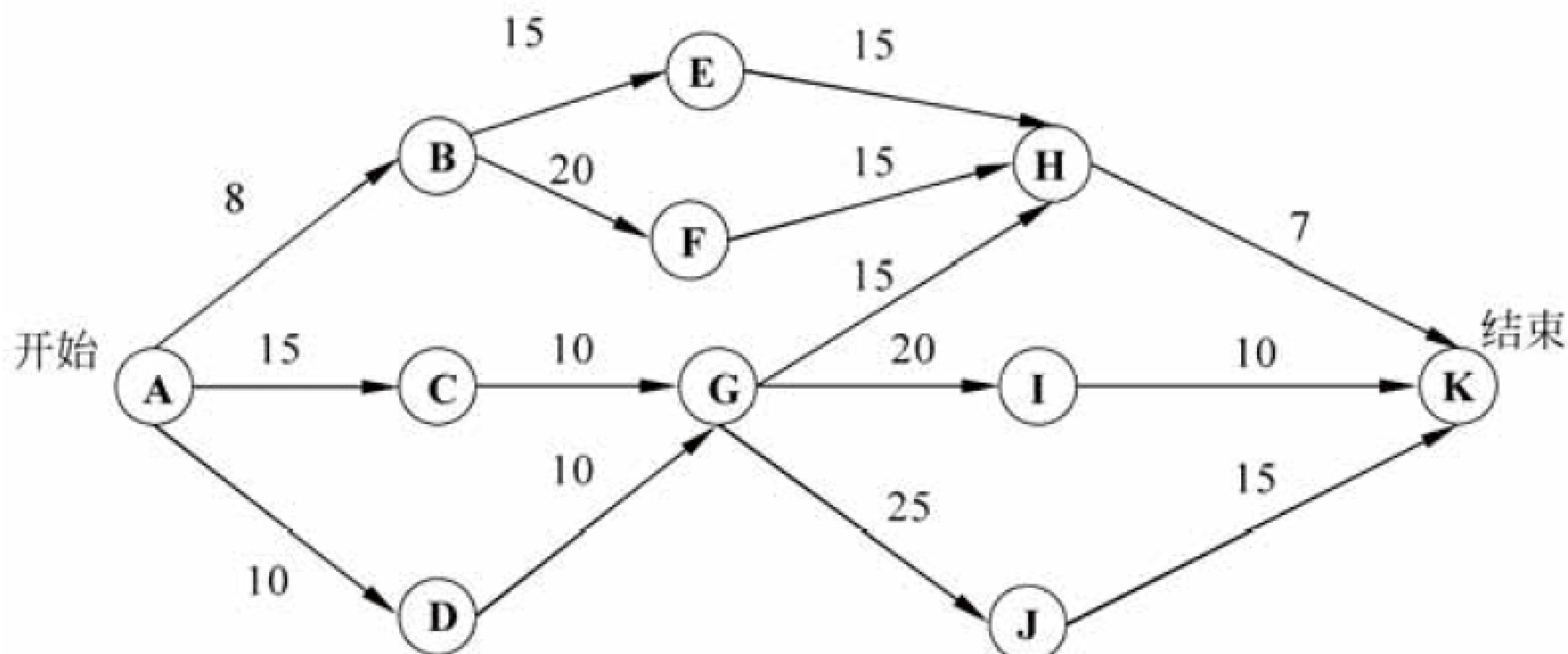
视频信息是指活动的、连续的图像序列。一幅图像称为一帧，帧是构成视频信息的基本单元。

**参考答案**

（5）A

**试题（6）、（7）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑__（6）__在关键路径上。若在实际项目进展中，活动 AD 在活动 AC 开始 3 天后才开始，而完成活动 DG 过程中，由于有临时事件发生，实际需要 15 天才能完成，则完成该项目的最短时间比原计划多了__（7）__天。



（6）A．B　　B．C　　C．D　　D．I

（7）A．8　　B．3　　C．5　　D．6

**试题（6）、（7）分析**

本题考查软件项目管理的基础知识。

根据关键路径法，计算出关键路径为 A→C→G→I→K，关键路径长度为 65。因此里程碑 C 在关键路径上，而里程碑 B、D 和 I 不在关键路径上。

若完成活动 DG 需要 15 天，则相当于 A→D→G→I→K 也是一个关键路径，而且活动 AD 推迟了三天才能完成，此时，完成项目的最短时间应该是 68 天，比原来的最短时间 65 天多了 3 天。

**参考答案**

（6）B　（7）B

**试题（8）**

为说明某一问题，在学术论文中需要引用某些资料。以下叙述中错误的是__（8）__。

（8）A．既可引用发表的作品，也可引用未发表的作品

B．只能限于介绍、评论作品

C．只要不构成自己作品的主要部分，可适当引用资料

D．不必征得原作者的同意，不需要向他支付报酬

**试题（8）分析**

本题考查知识产权方面的基础知识。

选项 A“既可引用发表的作品，也可引用未发表的作品”的说法显然是错误的。因为，为说明某一问题，在学术论文中需要引用某些资料必须是已发表的作品，但只能限于介绍、评论作品，只要不构成自己作品的主要部分，可适当引用资料，而不必征得原作者的同意，不需要向他支付报酬。

**参考答案**

（8）A

**试题（9）**

程序运行过程中常使用参数在函数（过程）间传递信息，引用调用传递的是实参的__（9）__。

（9）A．地址　　B．类型　　C．名称　　D．值

**试题（9）分析**

本题考查程序语言基础知识。

进行函数调用时，常需要将调用环境中的数据传递给被调用函数，作为输入参数由被调用函数处理，基本的调用方式为值调用（或传值调用）和引用调用。其中，值调用方式下是将实参的值单向地传递给被调用函数的形参，引用调用方式下通过将实参的地址传递给形参，在被调用函数中通过指针实现对实参变量数据的间接访问和修改，从而

达到将修改后的值“传回来”的效果。

**参考答案**

（9）A

**试题（10）**

算术表达式 a+(b-c)*d 的后缀式是<u>（10）</u>（–、+、*表示算术的减、加、乘运算，运算符的优先级和结合性遵循惯例）。

（10）A．b c – d * a +　　　　B．a b c – d * +

C．a b + c – d *　　　　D．a b c d –* +

**试题（10）分析**

本题考查程序语言基础知识。

后缀式的特点是将运算符号写在运算数的后面。对于表达式，其计算次序是相减、相乘、相加，其后缀式为“abc–d*+”。

**参考答案**

（10）B

**试题（11）、（12）**

帧中继网络的虚电路建立在<u>（11）</u>，这种虚电路的特点是<u>（12）</u>。

（11）A．数据链路层　　　　B．网络层

C．传输层　　　　D．会话层

（12）A．没有流量控制功能，也没有拥塞控制功能

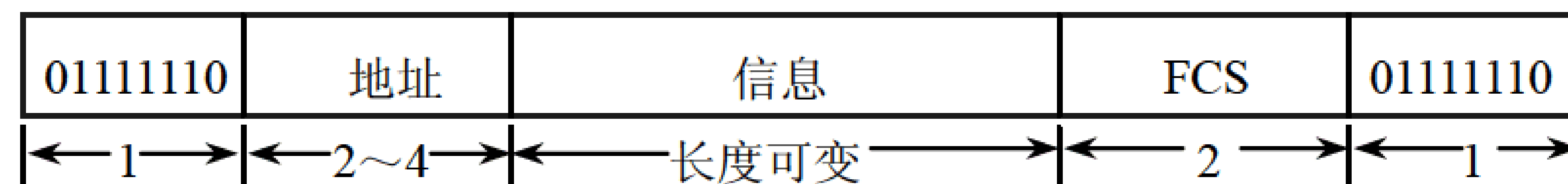
B．没有流量控制功能，但具有拥塞控制功能

C．具有流量控制功能，但没有拥塞控制功能

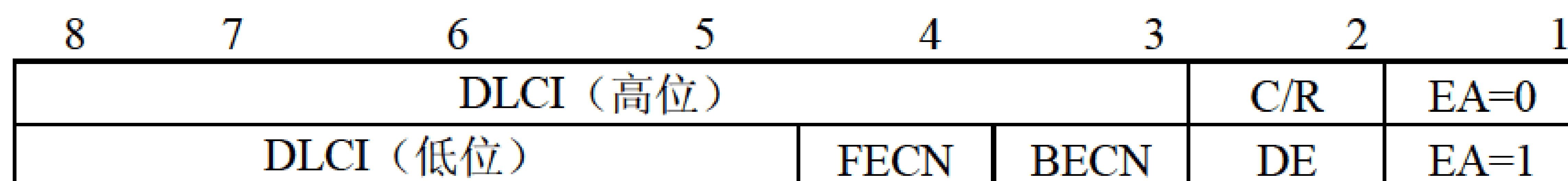
D．具有流量控制功能，也具有拥塞控制功能

**试题（11）、（12）分析**

帧中继（Frame Relay，FR）是作为综合业务数字网（ISDN）的一种承载业务而开发的。按照 ISDN 的体系结构，帧中继在第二层建立虚电路，用帧方式承载数据业务，因而第三层被省略了。在用户平面，通过 LAP-F(Q.922)帧传送用户数据。LAP-F 类似于 LAP-B，但是省去了控制字段，其帧格式如下图所示。




（a）帧格式



| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| DLCI（高位） | | | | | | C/R | EA=0 |
| DLCI（低位） | | | | FECN | BECN | DE | EA=1 |

（b）2 字节地址格式

图　帧中继的帧格式

从图 1 可以看出，帧头和帧尾都是一个字节的帧标志字段，其编码为“01111110”，与 HDLC 一样。信息字段长度可变，默认的最大长度是 1600 字节。帧效验序列也与 HDLC 相同，但是中间系统并不进行差错校验，只是接收端才用这个字段对整个帧进行校验。RF 没有流量控制功能，表现在帧结构上是没有发送顺序号和接收顺序号字段。地址字段有 3 种格式，图 1 所示为 2 字节地址格式，其中的 DLCI 为虚电路号，FECN 和 BECN 分别为向前拥塞和向后拥塞控制字段，而 DE 为 1 时表示优先丢弃，帧中继用这些机制实现拥塞控制。

**参考答案**

（11）A　（12）B

**试题（13）、（14）**

循环冗余校验标准 CRC-16 的生成多项式为 $G(x)=x^{16}+x^{15}+x^2+1$，它产生的校验码是<u>（13）</u>位。接收端发现错误后采取的措施是<u>（14）</u>。

（13）A．2　　B．4　　C．16　　D．32

（14）A．自动纠错　　B．报告上层协议

　　　C．重新生成数据　　D．自动请求重发

**试题（13）、（14）分析**

CRC-16 的 G(x)为 x 的十六次方多项式，所以产生的校验码是 16 位。CRC 校验属于后向纠错（Backward Error Correction，BEC），接收端发现错误后自动请求发送方重新发送数据。相反，对于前向纠错（Forward Error Correction，FEC），则是由接收端利用纠错码自动进行检查和纠正错误。

**参考答案**

（13）C　（14）D

**试题（15）**

设信道带宽为 3000Hz，信噪比为 30dB，则信道可达到的最大数据速率约为<u>（15）</u>b/s。

（15）A．10000　　B．20000　　C．30000　　D．40000

**试题（15）分析**

按照香农（Shannon）定理，噪声信道的极限数据速率由下面的公式计算：

本题中，$W$=3000Hz，信噪比为 30dB，即 $S/N$=1000，所以

$C=3000\times\log_2(1+1000)\approx 30000$b/s。

**参考答案**

（15）C

**试题（16）**

下面哪个字段包含在 TCP 头部和 UDP 头部？＿（16）＿

（16）A．发送顺序号　　　　B．窗口

C．源端口　　　　D．紧急指针

**试题（16）分析**

TCP 段头如下图 1 所示，UDP 头如下图 2 所示，可以看出，只有源端口字段出现在两个头部中。

<table>
<tr><td colspan="4">源端口</td><td colspan="5">目标端口</td></tr>
<tr><td colspan="9">发送顺序号</td></tr>
<tr><td colspan="9">接收顺序号</td></tr>
<tr><td>偏置值</td><td>保留</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>窗口</td></tr>
<tr><td colspan="8">检查和</td><td>紧急指针</td></tr>
<tr><td colspan="9">任选项+补丁</td></tr>
<tr><td colspan="9">用户数据</td></tr>
</table>

图 1　TCP 段头格式

| 源端口 | 目标端口 |
|---|---|
| 段　长 | 检查和 |

图 2　UDP 头

**参考答案**

（16）C

**试题（17）、（18）**

下面的选项中，与服务质量管理有关的协议是＿（17）＿，这种协议的主要特点是＿（18）＿。

（17）A．RSVP　　B．VTP　　C．ATM　　D．UDP

（18）A．由接收方向路由器预约资源　　B．由发送方向接收方预约资源

C．由发送方向路由器预约资源　　D．由接收方向发送方预约资源

**试题（17）、（18）分析**

本题的选项中，RSVP 是资源预约协议，根据用户要求的服务质量，由连接的接收方（或下游结点）向中间路由器（或上游结点）预约资源。VTP 是 VLAN 中继协议（VLAN Trunking Protocol），用于交换机之间共享 VLAN 配置信息，ATM 是一种信元交换网，而 UDP 是传输层协议，这些都与服务质量无关。

**参考答案**

（17）A　（18）A

**试题（19）、（20）**

CHAP 协议是 PPP 链路中采用的一种身份认证协议，这种协议采用__（19）__握手方式周期性地验证通信对方的身份，当认证服务器发出一个挑战报文时，则终端就计算该报文的__（20）__并把结果返回服务器。

（19）A. 两次　　B. 三次　　C. 四次　　D. 周期性

（20）A. 密码　　B. 补码　　C. CHAP 值　　D. HASH 值

**试题（19）、（20）分析**

PPP 认证协议是可选的，分为两种。

口令验证协议（Password Authentication Protocol，PAP）提供了一种简单的两次握手认证方法，由终端发送用户标识和口令字，等待服务器的应答，如果认证不成功，则终止连接。这种方案采用明文方式发送密码，可能会被第三方窃取。

质询握手认证协议（Challenge Handshake Authentication Protocol，CHAP）采用三次握手方式周期地验证对方的身份。PPP 链路建立后，认证服务器首先发送一个挑战报文（随机数），终端计算该报文的 Hash 值并把结果返回服务器，然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较，如果匹配，则认证通过，否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与，而密钥是不通过网络传送的，所以 CHAP 是更安全的认证机制。在后续的通信过程中，每经过一个随机的间隔，这个认证过程都可能被重复，以缩短入侵者进行持续攻击的时间。

**参考答案**

（19）B　（20）D

**试题（21）、（22）**

IP 头和 TCP 头的最小开销合计为__（21）__字节，以太网最大帧长为 1518 字节，则可以传送的 TCP 数据最大为__（22）__字节。

（21）A. 20　　B. 30　　C. 40　　D. 50

（22）A. 1434　　B. 1460　　C. 1480　　D. 1500

**试题（21）、（22）分析**

IP 头最少 20 个字节（不计任选字段），TCP 头最少也是 20 个字节（不计任选字段），最小合计 40 个字节。以太网帧最大负载长度为 1500 字节，另外帧头和帧尾还有 18 个字节。封装在以太帧中的 TCP 数据最多可以为 1460 字节。

**参考答案**

（21）C　（22）B

**试题（23）～（25）**

VLAN 中继协议（VTP）的作用是__（23）__。按照 VTP 协议，交换机的运行模式有__（24）__。如果要启动 VTP 动态修剪，则__（25）__。

（23）A. 启动 VLAN 自动配置过程

B. 减少 VLAN 配置信息的冲突
C. 让同一管理域中的所有交换机共享 VLAN 配置信息
D. 建立动态配置 VLAN 的环境

（24）A. 服务器模式，客户机模式，透明模式
B. 服务器模式，客户机模式，终端模式
C. 路由器模式，交换机模式，终端模式
D. 路由器模式，交换机模式，透明模式

（25）A. 管理域中的交换机必须配置成一个服务器和多个客户机
B. 管理域中的所有交换机都不能配置成终端模式
C. 管理域中的所有交换机都不能配置成透明模式
D. 管理域中的所有交换机都必须配置成服务器

**试题（23）～（25）分析**

VLAN 中继协议（VLAN Trunking Protocol，VTP）是 Cisco 公司的专利协议。按照 VTP 协议，交换机的运行模式分为 3 种：

① 服务器模式（Server）：在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。

② 客户机模式（Client）：在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

③ 透明模式（Transparent）：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能根据 VTP 帧更新自己的 VLAN 配置。

通过 VTP 协议，提供了在一台交换机上对整个管理域（跨不同介质类型）进行 VLAN 配置的方法，使得同一管理域中的所有交换机共享 VLAN 配置信息。

在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛到所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。为了解决这个问题，可以使用静态或动态修剪的方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪方式容易出错，并且对任何 VLAN 配置的变化，都必须重新进行手工修剪。VTP 动态修剪允许交换机从中继连接上自动剪掉不活动的 VLAN，使得中继链路上共享的 VLAN 都是活动的。

动态修剪要求 VTP 域中的所有交换机都必须配置成服务器。因为在服务器模式下，交换机可以改变 VLAN 配置，也可以接受 VLAN 配置的改变。

**参考答案**

（23）C　（24）A　（25）D

**试题（26）、（27）**

在下面的标准中，定义快速生成树协议的是__（26）__，支持端口认证的协议是__（27）__。

（26）A．IEEE802.1d　　B．IEEE802.1w
　　　C．IEEE802.1s　　D．IEEE802.1x

（27）A．IEEE802.1d　　B．IEEE802.1w
　　　C．IEEE802.1s　　D．IEEE802.1x

**试题（26）、（27）分析**

生成树协议（STP）删除了交换机之间的网络环路，同时允许一定的冗余连接存在，以增加带宽，提高网络连接的可靠性。1990 年，IEEE 根据 DEC 公司的 STP 协议开发了 802.1d 标准。

1998 年，IEEE 颁布了快速生成树协议（RSTP）802.1w，这种协议在网络拓扑改变时可以加快生成树收敛的速度。在原来的 STP 协议中，生成树的收敛时间可能达到 30～50 秒，而 RSTP 的收敛时间通常只有 6 秒钟（默认 hello times=2 秒）。最新的 IEEE802.1d-2004 标准包含了 RSTP 的内容，废除了原来的 STP 协议。

如果交换是以太网中有多个 VLAN 存在，可以为每个 VLAN 配置一个生成树。多生成树协议（Multiple Spanning Tree Protocol，MSTP）是 RSTP 在 VLAN 环境下的扩展，原来定义在 IEEE 802.1s 中，后来被合并到新标准 IEEE 802.1q-2003 中。这种“每个 VLAN 的多生成树协议”为每一组 VLAN 配置一个单独的生成树，并预留一个可用的替代通路，而将其他通路置于阻塞状态。MSTP 在一个 MST 区域中通过传播通知信息而维护多个 MST 实例。多个 MST 区域（或者其他的 STP 网桥）之间则通过公共生成树（common spanning tree，CST）互连，CST 就是 STP 协议的生成树。MSTP 协议把所有生成树信息包装在单一的 BPDU 格式中，并且保证与 STP 和 RSTP 协议向后兼容，所以 RSTP 网桥也可以解释 MSTP 的 BPDU。

IEEE 802.1x 在局域网中实现基于端口的用户认证和访问控制。

**参考答案**

（26）B　（27）D

**试题（28）**

在某路由器上查看路由信息，结果如下所示。其中标志 “S”表明这条路由是__（28）__。

```
        192.168.0.0/24 is subnetted, 1subnets
S       192.168.1.0 [1/0] via 10.1.1.1
                  10.0.0.0/24 is subnetted, 1subnets
C       10.1.1.0 is directly connected, Ethernet0
```

（28）A．源路由　　　　B．静态路由

　　　C．发送路由　　　D．快捷路由

**试题（28）分析**

本题考查路由器配置命令。查看路由信息结果中，标记 S 表示静态路由，标记 C 表示直联，标记 R 表示采用 RIP 路由协议。

**参考答案**

（28）B

**试题（29）、（30）**

下图中第 23 条记录是某客户机收到的 TCP 报文，从结果中可以看出该客户机的 IP 地址为 （29） ，该 TCP 报文是 （30） 。

```
111  [Wireshark 1.7.0 (SVN Rev 39768 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:                                  Expression... Clear Apply Save
No. Time       Source          Destination     Protocol Length Info
 21 3.86991600 219.245.67.193  255.255.255.255 UDP      82 Source port: eristwoguns  Destination port: sentine
 22 4.36134900 219.245.67.185  219.245.67.255  NBNS     92 Name query NB ISATAP<00>
 23 4.96058400 218.30.66.226   219.245.67.39   TCP      60 http > 1895 [FIN, ACK] Seq=1 Ack=1 Win=65 Len=0
 24 4.96066500 219.245.67.39   218.30.66.226   TCP      54 1895 > http [ACK] Seq=1 Ack=2 Win=65535 Len=0
 25 5.09693800 219.245.67.39   218.30.66.226   TCP      54 1895 > http [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

⊞ Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Hangzhou_1a:06:7c (00:23:89:1a:06:7c), Dst: Giga-Byt_39:62:3e (00:1d:7d:39:62:3e)
⊞ Internet Protocol Version 4, Src: 218.30.66.226 (218.30.66.226), Dst: 219.245.67.39 (219.245.67.39)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 1895 (1895), Seq: 1, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 1895 (1895)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x011 (FIN, ACK)
    Window size value: 65
    [Calculated window size: 65]
    [Window size scaling factor: -1 (unknown)]
  ⊞ Checksum: 0x070d [validation disabled]

0000  00 1d 7d 39 62 3e 00 23  89 1a 06 7c 08 00 45 00   ..}9b>.# ...|..E.
0010  00 28 5d 99 00 00 36 06  eb 19 da 1e 42 e2 db f5   .(]...6. ....B...
0020  43 27 00 50 07 67 e3 10  d0 bc c0 d2 f0 10 50 11   C'.P.g.. ......P.
0030  00 41 07 0d 00 00 00 00  00 00 00 00               .A...... ....

Flags (tcp.flags), 2 bytes | Packets: 2762 Displayed: 2762 Marked: 0 Load time: 0:01.515 | Profile: Default
```

（29）A．218.30.66.266　　　　B．219.245.67.39

　　　C．219.245.67.185　　　D．219.245.67.193

（30）A．连接建立请求报文　　　B．错误复位报文

　　　C．连接建立响应报文　　　D．连接断开响应报文

**试题（29）、（30）分析**

本题考查网络管理工具的使用和报文格式。由第 23 条记录是某客户机收到的 TCP 报文，故报文的目的 IP 地址为本机地址，即 219.245.67.39；再由标志字段 FIN 和 ACK 为真，故该报文为连接断开响应报文。

**参考答案**

（29）B　（30）D

**试题（31）**

在 Linux 操作系统中把外部设备当作文件统一管理，外部设备文件通常放在__（31）__目录中。

（31）A．/dev　　B．/lib　　C．/etc　　D．/bin

**试题（31）分析**

本题考查 Linux 操作系统中的目录。

/dev 目录中包含了所有 Linux 系统中使用的外部设备，但不存放外部设备驱动程序；/lib 目录里存放着系统最基本的动态链接共享库，其作用类似于 Windows 里的.dll 文件；/etc 主要存放了系统配置方面的文件；/bin 目录存放了标准的（或者说是缺省的）linux 的工具，比如像“ls”、“vi”还有“more”等等。

**参考答案**

（31）A

**试题（32）**

Linux 中，下列__（32）__命令可以更改一个文件的权限设置。

（32）A．attrib　　B．file　　C．chmod　　D．change

**试题（32）分析**

本题考查 Linux 操作系统中的文件及其权限。

Attrib 是 Windows 中给文件加系统属性的命令；

file 是 Linux 操作系统中检测文件类型的命令；

chmod 是 Linux 操作系统中赋予权限的命令，使用方式为：chmod [-cfvR] [--help] [--version] mode file...。

**参考答案**

（32）C

**试题（33）**

以下关于 DNS 服务器的说法中，错误的是__（33）__。

（33）A．DNS 的域名空间是由树状结构组织的分层域名

B．转发域名服务器位于域名树的顶层

C．辅助域名服务器定期从主域名服务器获得更新数据

D．转发域名服务器负责所有非本地域名的查询

**试题（33）分析**

本题考查 DNS 服务器相关概念。

域名系统通过层次结构的分布式数据库建立了一致性的名字空间，用来定位网络资源。DNS 的逻辑结构是一个分层的域名树，Internet 网络信息中心管理着域名树的根，

称为根域。根域下面是顶级域，分为国家顶级域和通用顶级域。国家顶级域名包含 243 个国家和地区代码，例如 cn 代表中国，uk 代表英国等。

转发域名服务器负责所有非本地域名的查询。当 DNS 服务器收到查询请求后，首先在自己的区域文件中查找，再在高速缓存中查找。如果查不到，可能是因为该服务器不是请求域的授权服务器，并且以前查询的缓存中没有需要的记录，这时 DNS 服务器必须向转发域名服务器发送请求。

当主域名服务器关闭、出现故障或负载过重时，辅助域名服务器作为备份服务器提供域名解析服务。辅助服务器从主域名服务器获得授权，并定期向主服务器询问是否有新数据，如果有则调入并更新域名解析数据，以达到与主域名服务器同步的目的。

**参考答案**

（33）B

**试题（34）**

某单位架设了域名服务器来进行本地域名解析，在客户机上运行 nslookup 查询某服务器名称时能解析出 IP 地址，查询 IP 地址时却不能解析出服务器名称，解决这一问题的方法是__（34）__。

（34）A．在 DNS 服务器区域上允许动态更新

B．在客户机上采用 ipconfig/flushdns 刷新 DNS 缓存

C．在 DNS 服务器上为该服务器创建 PTR 记录

D．重启 DNS 服务

**试题（34）分析**

本题考查 DNS 服务相关知识。

查询服务器名称时能解析出 IP 地址，而查询 IP 地址时却不能解析出服务器名称，说明可正向解析不能反向解析，因此须在 DNS 服务器上为该服务器创建反向解析（PTR）记录。

**参考答案**

（34）C

**试题（35）**

下列关于 DHCP 配置的叙述中，错误的是__（35）__。

（35）A．在 Windows 环境下，客户机可用命令 ipconfig /renew 重新申请 IP 地址

B．若可供分配的 IP 地址较多，可适当增加地址租约期限

C．DHCP 服务器不需要配置固定的 IP 地址

D．DHCP 服务器可以为不在同一网段的客户机分配 IP 地址

**试题（35）分析**

本题考查 DHCP 服务器配置相关知识。

在 Windows 环境下，客户机可用命令 ipconfig /release 释放 IP 地址，用命令 ipconfig

/renew 重新申请 IP 地址；在 DHCP 服务器的地址租约期限设置中，可依据可供分配 IP 地址的多少，适当调整地址租约期限；DHCP 服务器需要有固定的 IP 地址，便于和客户机之间通过 DHCP 协议报文分配 IP 地址；可以通过在路由器上设置中继代理，为不在同一网段的客户机分配 IP 地址。

**参考答案**

（35）C

**试题（36）**

SMTP 协议用于__（36）__电子邮件。

（36）A．接收　　B．发送　　C．丢弃　　D．阻挡

**试题（36）分析**

本题考查 SMTP 协议的功能。

SMTP 协议的功能是发送电子邮件，PoP3 协议的功能是接收电子邮件。

**参考答案**

（36）B

**试题（37）**

配置 POP3 服务器时，邮件服务器中默认开放 TCP 的__（37）__端口。

（37）A．21　　B．25　　C．53　　D．110

**试题（37）分析**

本题考查 POP3 协议的相关知识。

不同的协议采用不同的 TCP 端口号，默认情况下，Web 服务器的端口号为 80；FTP 服务器的端口号为 20 和 21，Telnet 的端口号为 25，POP3 的端口号为 110。

**参考答案**

（37）D

**试题（38）**

在 Windows 的 cmd 命令窗口中输入__（38）__命令可以用来诊断域名系统基础结构的信息和查看 DNS 服务器的 IP 地址。

（38）A．DNSserver　B．DNSconfig　C．Nslookup　D．DNSnamed

**试题（38）分析**

本题考查 Windows 操作系统中网络管理命令的使用及相关知识。

通常采用 Nslookup 命令来诊断域名系统基础结构的信息和查看 DNS 服务器的 IP 地址。

**参考答案**

（38）C

**试题（39）**

计算机网络机房建设过程中，为了屏蔽外界的干扰、漏电及电火花等，要求所有计

算机网络设备的机箱、机柜、机壳等都需接地，该接地系统称为安全地，安全地接地电阻要求小于__（39）__。

（39）A．1Ω　　B．4Ω　　C．5Ω　　D．10Ω

**试题（39）分析**

本题考查机房建设过程中需注意的问题。

通常标准接地电阻规范要求：

① 独立的防雷保护接地电阻应小于等于 10Ω；

② 独立的安全保护接地电阻应小于等于 4Ω；

③ 独立的交流工作接地电阻应小于等于 4Ω；

④ 独立的直流工作接地电阻应小于等于 4Ω；

⑤ 防静电接地电阻一般要求小于等于 100Ω；

⑥ 共用接地体（联合接地）应不大于接地电阻 1Ω。

**参考答案**

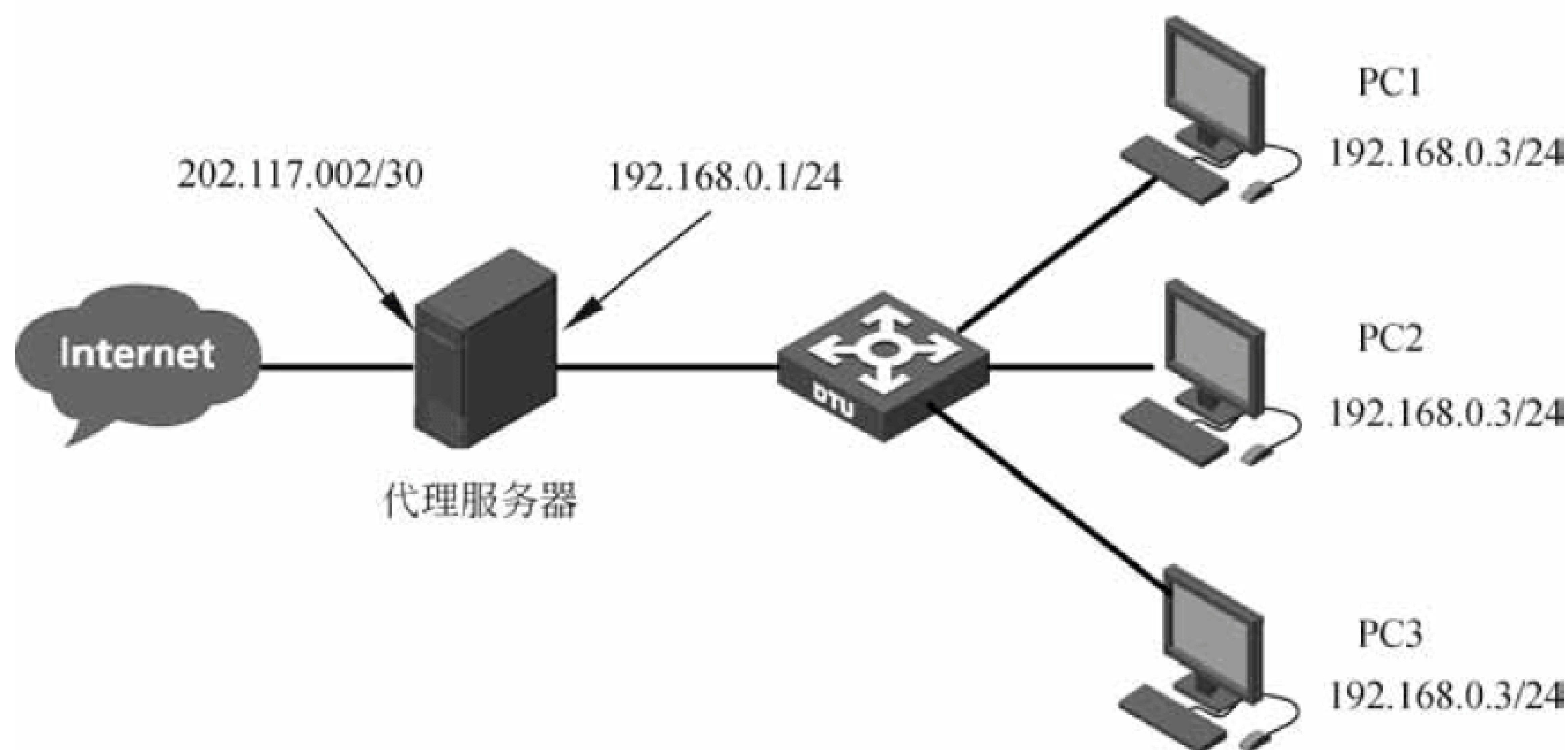
（39）B

**试题（40）**

某单位局域网配置如下图所示，PC2 发送到 Internet 上的报文源 IP 地址为__（40）__。

（40）A．192.168.0.2　　B．192.168.0.1

C．202.117.112.1　　D．202.117.112.2




**试题（40）分析**

本题考查局域网配置中 IP 地址设置相关问题。

PC2 发送到 Internet 上的报文经代理服务器转换后，源 IP 地址变成代理服务器的出口 IP 地址，即 202.117.112.2。

**参考答案**

（40）D

**试题（41）**

下面 ACL 语句中，表达“禁止外网和内网之间互相 ping”的是__（41）__。

（41）A．access-list 101 permit　any　any
　　B．access-list 101 permit　icmp　any　any
　　C．access-list 101 deny　any　any
　　D．access-list 101 deny　icmp　any　any

**试题（41）分析**

本题考查 ACL 语句规范及 ICMP 命令。

Ping 命令是 ICMP 报文的一个子集，禁止内外网用户之间采用 ICMP 协议即可禁止外网和内网之间互相 ping。

**参考答案**

（41）D

**试题（42）**

下列网络攻击行为中，属于 DoS 攻击的是__（42）__。

（42）A．特洛伊木马攻击　　B．SYN Flooding 攻击
　　C．端口欺骗攻击　　D．IP 欺骗攻击

**试题（42）分析**

本题考查网络安全相关知识。

特洛伊木马是附着在应用程序中或者单独存在的一些恶意程序，它可以利用网络远程控制网络另一端的安装有服务端程序的主机，实现对被植入了木马程序的计算机的控制，或者窃取被植入了木马程序的计算机上的机密资料。

拒绝服务攻击通过网络的内外部用户来发动攻击。内部用户可以通过长时间占用系统的内存、CPU 处理时间使其他用户不能及时得到这些资源，而引起拒绝服务攻击；外部黑客也可以通过占用网络连接使其他用户得不到网络服务。SYN Flooding 攻击以多个随机的源主机地址向目的路由器发送 SYN 包，在收到目的路由器的 SYN ACK 后并不回应，于是目的路由器就为这些源主机建立大量的连接队列，由于没有收到 ACK 一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务,甚至导致路由器崩溃。服务器要等待超时才能断开已分配的资源，所以 SYN Flooding 攻击是一种 DoS 攻击。

端口欺骗攻击是采用端口扫描找到系统漏洞从而实施攻击。

IP 欺骗攻击是产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。

**参考答案**

（42）B

**试题（43）**

PKI 体制中，保证数字证书不被篡改的方法是＿（43）＿。

（43）A．用 CA 的私钥对数字证书签名
　　B．用 CA 的公钥对数字证书签名
　　C．用证书主人的私钥对数字证书签名
　　D．用证书主人的公钥对数字证书签名

**试题（43）分析**

本题考查 PKI 体制。

PKI 体制中，为保障数字证书不被篡改而且要发送到证书主人手中，需要用 CA 的私钥对数字证书签名，防伪造，不可抵赖。

**参考答案**

（43）A

**试题（44）**

报文摘要算法 SHA-1 输出的位数是＿（44）＿。

（44）A．100 位　　B．128 位　　C．160 位　　D．180 位

**试题（44）分析**

本题考查报文摘要算法 SHA-1。

SHA-1 从一个最大 $2^{64}$ 位的信息中产生一串 160 位的摘要。

**参考答案**

（44）C

**试题（45）**

下面算法中，不属于公开密钥加密算法的是＿（45）＿。

（45）A．ECC　　B．DSA　　C．RSA　　D．DES

**试题（45）分析**

本题考查加密算法的基础知识。

常用的加密算法依据所使用的秘钥数分为单钥和双钥加密体制，也称私钥和公钥加密算法。ECC、DSA 和 RSA 都属于公开密钥加密算法，DES 是典型的私钥加密体制。

**参考答案**

（45）D

**试题（46）**

在 DHCP 服务器配置过程中，可以把使用 DHCP 协议获取 IP 地址的主机划分为不同的类别进行管理，下面划分类别规则合理的是＿（46）＿。

（46）A．移动用户划分到租约期较长的类别
　　B．固定用户划分到租约期较短的类别
　　C．服务器划分到租约期最短的类别

D. 服务器可以采用保留地址

**试题（46）分析**

本题考查 DHCP 服务器配置的基础知识。

DHCP 服务器分配 IP 地址时，默认租约期限为 8 天，租约到期前客户端若需要续订，续订工作由客户端自动完成。如果网络中有较多可用的 IP 地址并且很少对配置进行更改，则增加租约期限长度可以减少客户端和 DHCP 服务器之间的租约续订查询的频率。这将会减少由客户端续订租约引起的一些网络通信量。如果网络上可用的 IP 地址数量较少并且经常更改客户端配置或客户端移动频繁，则应减少租约期限，以促进 DHCP 服务器对过时 IP 地址的清理工作。

一般来说，对于移动用户设置较短的租约期限较好，对于固定用户设置较长的租约期限较好。服务器一般不能随便更改 IP 地址，所以在配置 DHCP 服务器时，一般为服务器保留特定的 IP 地址。

**参考答案**

（46）D

**试题（47）**

在某公司局域网中的一台 Windows 主机中，先运行＿（47）＿命令，再运行“arp -a”命令，系统显示的信息如下图所示。

```
C:\>arp -a

Interface:192.168.1.1 --- 0x20002
  Internet Address      Physical Address        Type
  192.168.1.1           00-23-8b-be-60-37        dynamic
  192.168.1.2           01-00-5e-06-38-24        dynamic
  192.168.1.3           00-00-00-00-00-00        invalid
  192.168.1.254         00-22-15-f2-6b-ea        static
```

（47）A. arp -s 192.168.1.1 00-23-8b-be-60-37

B. arp -s 192.168.1.2 01-00-5e-06-38-24

C. arp -s 192.168.1.3 00-00-00-00-00-00

D. arp -s 192.168.1.254 00-22-15-f2-6b-ea

**试题（47）分析**

本题考查 Windows 系统的基本命令。

在 Windows 系统的命令行中，运行“arp-a”命令可以主机 ARP 缓存中的 IP 地址以及 MAC 地址的对应关系，“arp-s”命令用于绑定 ARP 缓存中的某个 IP 地址以及 MAC 地址对，对于某一个绑定的 IP 地址及 MAC 地址对，在 ARP 缓存表中“Type”项的值将由“dynamic”改为“static”。

“arp-s”命令的参数为“-s InetAddr EtherAddr [IfaceAddr]”，根据图中所给的系统提示信息，答案应为 D 选项。

**参考答案**

（47）D

**试题（48）**

SNMPc 软件支持的 4 个内置 TCP 服务是__（48）__。

（48）A．FTP、SMTP、WEB 和 TELNET

B．DHCP、SMTP、WEB 和 TELNET

C．DNS、SMTP、WEB 和 TELNET

D．TFTP、SMTP、WEB 和 TELNET

**试题（48）分析**

本题考查网络管理软件 SNMPc 的基本知识。

SNMPc 是一个通用的分布式的网络管理平台，可以轮询定制的 TCP 应用服务和 4 个内置的 TCP 应用服务(FTP、SMTP、WEB 和 TELNET)。

**参考答案**

（48）A

**试题（49）**

在 MIB-2 的系统组中，__（49）__对象以 7 位二进制数表示，每一位对应 OSI/RM 7 层协议中的一层。

（49）A．sysDescr　　B．sysUpTime

C．sysName　　D．sysServices

**试题（49）分析**

本题考查管理信息库第二版的有关系统组的内容。

系统组提供了系统的一般信息，系统服务对象 sysServices 是 7 位二进制数，每一位对应 OSI/RM7 层协议中的一层。如果系统提供某一层服务，则对应的位为 1，否则为 0。

**参考答案**

（49）D

**试题（50）**

SNMPv2 提供了几种访问管理信息的方法，其中属于 SNMPv2 特有的是__（50）__。

（50）A．管理站与代理之间的请求/响应通信

B．管理站与管理站之间的请求/响应通信

C．代理到管理站的非确认通信

D．代理向管理站发送陷入报文

**试题（50）分析**

SNMPv2 提供了 3 种访问管理信息的方法：一是管理站与代理之间的请求/响应通信，这种方法与 SNMPv1 是一样的；二是管理站与管理站之间的请求/响应通信，这种方法是 SNMPv2 特有的，可以由一个管理站把有关管理信息告诉另一个管理站；三是代理到

管理站的非确认通信，即由代理向管理站发送陷入报文，报告出现的异常情况，SNMPv1 中也有对应的通信方式。

**参考答案**

（50）B

**试题（51）**

属于网络 202.115.200.0/21 的地址是__（51）__。

（51）A．202.115.198.0　　B．202.115.206.0
　　C．202.115.217.0　　D．202.115.224.0

**试题（51）分析**

网络地址 202.115.200.0/21 的二进制是：　**11001010.01110011.11001**000.00000000
网络地址 202.115.198.0 的二进制是：　11001010.01110011.11000110.00000000
网络地址 202.115.206.0 的二进制是：　**11001010.01110011.11001**110.00000000
网络地址 202.115.217.0 的二进制是：　11001010.01110011.11011001.00000000
网络地址 202.115.224.0 的二进制是：　11001010.01110011.11100000.00000000

可见，能与网络地址 202.115.200.0/21 达到最长匹配的是 202.115.206.0

**参考答案**

（51）B

**试题（52）**

4 条路由：220.117.129.0/24、220.117.130.0/24、220.117.132.0/24 和 220.117.133.0/24 经过汇聚后得到的网络地址是__（52）__。

（52）A．220.117.132.0/23　　B．220.117.128.0/22
　　C．220.117.130.0/22　　D．220.117.128.0/21

**试题（52）分析**

4 条路由的二进制形式分别是：

220.117.129.0/24　**11011100.01110101.10000001**.00000000
220.117.130.0/24　**11011100.01110101.10000010**.00000000
220.117.132.0/24　**11011100.01110101.10000100**.00000000
220.117.133.0/24　**11011100.01110101.10000101**.00000000

经过汇聚后得到的网络地址是：

220.117.128.0/21　**11011100.01110101.10000**000.00000000

**参考答案**

（52）D

**试题（53）、（54）**

某网络的地址是 200.16.0.0，其中包含 480 台主机，指定给该网络的合理子网掩码是__（53）__，下面的选项中，不属于这个网络的地址是__（54）__。

（53）A．255.255.255.0　　B．255.255.252.0
　　C．255.255.254.0　　D．255.255.248.0

（54）A．200.16.0.23　　B．200.16.3.0
　　C．200.16.1.255　　D．200.16.1.0

**试题（53）、（54）分析**

网络 200.16.0.0 中包含 480 台主机，其主机地址必须占 9 位，即其网络掩码为 255.255.254.0。

A．200.16.0.23　　**11001000. 00010000. 0000000**0. 00010111

B．200.16.3.0　　**11001000. 00010000. 0000001**1. 00000000

C．200.16.1.255　　**11001000. 00010000. 0000000**1. 11111111

D．200.16.1.0　　**11001000. 00010000. 0000000**1. 00000000

可以看出，A 是网络 200.16.0.0/23 中的主机地址，B 不是网络 200.16.0.0/23 中的地址。C 是 200.16.0.0/23 中的定向广播地址，D 是 200.16.0.0/23 中的主机地址。

**参考答案**

（53）C　（54）B

**试题（55）**

两个主机的 IP 地址分别是 10.11.7.24 和 10.11.7.100，要使得这两个主机包含在同一个子网中，则指定的子网掩码长度应该为__（55）__比特。

（55）A．25　　B．26　　C．27　　D．28

**试题（55）分析**

主机地址 10.11.7.24 的二进制形式是：　　**00001010. 00001011. 00000111. 0**0011000

主机地址 10.11.7.100 的二进制形式是：　　**00001010. 00001011. 00000111. 0**1100100

要使这两个主机地址包含在同一个子网中，指定的地址掩码最长为 25 位。

**参考答案**

（55）A

**试题（56）、（57）**

IPv6 链路本地单播地址的前缀为__（56）__，可聚集全球单播地址的前缀为__（57）__。

（56）A．001　　B．1111 1110 10　　C．1111 1110 11　　D．1111 1111

（57）A．001　　B．1111 1110 10　　C．1111 1110 11　　D．1111 1111

**试题（56）、（57）分析**

地址前缀 001 代表可聚集全球单播地址，地址前缀 1111 1110 10 代表链路本地单播地址，地址前缀 1111 1110 11 代表站点本地单播地址。IPv6 组播地址格式前缀为 1111 1111。

**参考答案**

（56）B　（57）A

**试题（58）、（59）**

在 IPv4 向 IPv6 的过渡期间，如果要使得两个 IPv6 结点可以通过现有的 IPv4 网络进行通信，则应该使用__（58）__；如果要使得纯 IPv6 结点可以与纯 IPv4 结点进行通信，则需要使用__（59）__。

（58）A．堆栈技术　B．双协议栈技术　C．隧道技术　D．翻译技术

（59）A．堆栈技术　B．双协议栈技术　C．隧道技术　D．翻译技术

**试题（58）、（59）分析**

如果要使得两个 IPv6 结点可以通过现有的 IPv4 网络进行通信，则应该使用隧道技术，如果要使得纯 IPv6 结点可以与纯 IPv4 结点进行通信，则需要使用翻译技术。

**参考答案**

（58）C　（59）D

**试题（60）**

以太网链路聚合技术是将__（60）__。

（60）A．多个逻辑链路聚合成一个物理链路

B．多个逻辑链路聚合成一个逻辑链路

C．多个物理链路聚合成一个物理链路

D．多个物理链路聚合成一个逻辑链路

**试题（60）分析**

IEEE 802.3ad 定义了链路聚合控制协议（Link Aggregation Control Protocol，LACP），它的功能是将多个物理链路聚合成一个逻辑链路。链路汇聚技术可以将多个链路绑定在一起，形成一条高速链路，以达到更高的带宽，并实现链路备份和负载均衡。

**参考答案**

（60）D

**试题（61）、（62）**

POP3 协议采用__（61）__模式进行通信，当客户机需要服务时，客户端软件与 POP3 服务器建立__（62）__连接。

（61）A．Browser/Server　B．Client/Server

C．Peer to Peer　D．Peer to Server

（62）A．TCP　B．UDP　C．PHP　D．IP

**试题（61）、（62）分析**

POP3 协议采用 C/S 模式进行通信，POP3 需要 TCP 连接的支持，当客户机需要服务时，客户端软件与 POP3 服务器建立 TCP 连接。

**参考答案**

（61）B　（62）A

**试题（63）～（65）**

TCP协议使用__（63）__次握手过程建立连接，这种方法可以防止__（64）__。TCP使用的流量控制协议是__（65）__。

（63）A. 一　　B. 二　　C. 三　　D. 四

（64）A. 出现半连接　　B. 出现错误连接
　　C. 假冒的连接　　D. 无法连接

（65）A. 固定大小的滑动窗口协议　　B. 可变大小的滑动窗口协议
　　C. 后退N帧ARQ协议　　D. 选择重发ARQ协议

**试题（63）～（65）分析**

TCP协议使用三次握手过程建立连接，这种方法可以防止出现错误连接。大部分错误连接是由于迟到的或网络中存储的连接请求引起的。由于三次握手过程强调连接的双方都要提出自己的连接请求标识，也要应答对方的连接请求标识，所以不会受到过期的连接请求的干扰。

TCP使用的流量控制协议是可变大小的滑动窗口协议，这种协议把肯定应答信号与扩大窗口的信号分开，更适合建立在不可靠网络上的远程连接使用。

**参考答案**

（63）C　（64）B　（65）B

**试题（66）、（67）**

IEEE 802.11 标准采用的工作频段是__（66）__，下列标准中采用双频工作模式的是__（67）__。

（66）A. 900MHz 和 800MHz　　B. 900MHz 和 2.4GHz
　　C. 5GHz 和 800MHz　　D. 2.4GHz 和 5GHz

（67）A. IEEE802.11a　　B. IEEE802.11b
　　C. IEEE802.11g　　D. IEEE802.11n

**试题（66）、（67）分析**

1997年颁布的IEEE 802.11标准运行在2.4GHz的ISM（Industrial Scientific and Medical）频段，1999年推出的IEEE 802.11a标准运行在5GHz的U-NII（Unlicensed National Information Infrastructure）频段，802.11b和802.11g也是运行在2.4GHz频段，2009年发布的802.11n标准则采用2.4GHz和5GHz双频工作模式。

**参考答案**

（66）D　（67）D

**试题（68）～（70）**

PC机不能接入因特网，这时采用抓包工具捕获的以太网接口发出的信息如下：

| Source | Destination | Protocol | Info |
|---|---|---|---|
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254?  Tell 213.127.115.31 |
| 213.127.115.31 | 213.127.115.255 | NBNS | Name query NB TRACKER9.BOL.BG<00> |
| 213.127.115.31 | 213.127.115.255 | NBNS | Name query NB BT.ROMMAN.NET<00> |
| 213.127.115.31 | 224.1.1.1 | UDP | Source port: ircu  Destination port: ircu |
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254?  Tell 213.127.115.31 |
| QuantaCo_33:9b:be | Broadcast | ARP | Who has 213.127.115.254?  Tell 213.127.115.31 |

可以看出该 PC 机的 IP 地址为__（68）__，默认网关的 IP 地址为__（69）__。PC 不能接入 Internet 的原因可能是__（70）__。

（68）A．213.127.115.31　　B．213.127.115.255
　　　C．213.127.115.254　　D．224.1.1.1

（69）A．213.127.115.31　　B．213.127.115.255
　　　C．213.127.115.254　　D．224.1.1.1

（70）A．DNS 解析错误　　B．TCP/IP 协议安装错误
　　　C．不能连接到网关　　D．DHCP 服务器工作不正常

**试题（68）～（70）分析**

由截图中的 ARP 广播包可以看出 PC 机的地址是 213.127.115.31，默认网关的地址是 213.127.115.254。截图信息显示 TCP/IP 协议安装正确，而且 DNS 服务器工作正常，所以 PC 机不能接入 Internet 的原因，只能选择“不能连接到网关”。

**参考答案**

（68）A　（69）C　（70）C

**试题（71）～（75）**

The de facto standard Application Program Interface (API) for TCP/IP applications is the "sockets" interface. Although this API was developed for __（71）__ in the early 1980s it has also been implemented on a wide variety of non-Unix systems. TCP/IP __（72）__ written using the sockets API have in the past enjoyed a high degree of portability and we would like the same __（73）__ with IPv6 applications. But changes are required to the sockets API to support IPv6 and this memo describes these changes. These include a new socket address structure to carry IPv6 __（74）__, new address conversion functions, and some new socket options. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete __（75）__ for existing IPv4 applications.

（71）A．Windows　　B．Linux　　C．Unix　　D．DOS

（72）A．applications　　B．networks　　C．protocols　　D．systems

（73）A．portability　　B．availability　　C．capability　　D．reliability

（74）A．connections B．protocols C．networks D．addresses

（75）A．availability B．compatibility C．capability D．reliability

**参考译文**

对于 TCP/IP 应用，事实上的应用程序接口（API）标准是“套接字”口。虽然这个 API 是在 1980 年代早期为 Unix 开发的，但是也广泛的在各种非 Unix 系统中得到了实现。以前采用套接字 API 编写的 TCP/IP 应用具有高度的兼容性，因而我们也希望对 IPv6 应用也具有同样的兼容性。为了支持 IPv6，需要对套接字 API 作出某些改变，这个便笺就是描述这些变化的。这些改变包括一种新的用于支持 IPv6 地址的套接字地址结构、新的地址转换功能以及新的套接字选项。这些扩展可以满足 TCP 和 UDP 应用访问 IPv6 基本功能（包括组播）时的需要，但是只对系统进行了最小的改变，而且与现有的 IPv4 应用是完全兼容的。

**参考答案**

（71）C （72）A （73）A （74）D （75）B

# 第 20 章　2013 下半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某省运营商的社区宽带接入网络结构如图 1-1 所示。

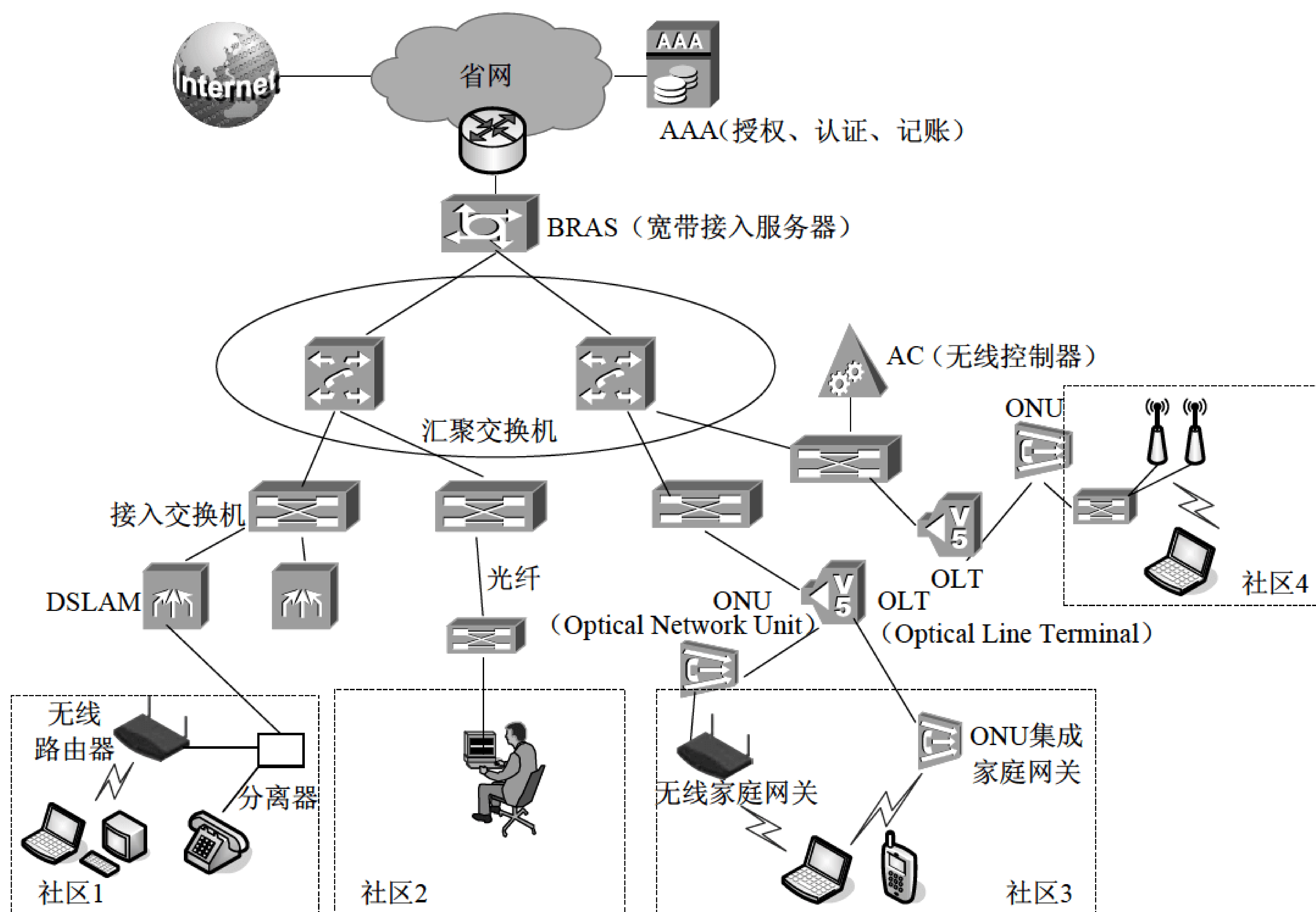



图 1-1

**【问题 1】（7 分）**

高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。图 1-1 所示的四个社区采用的小区宽带接入方法分别是：社区 1___（1）___，社区 2___（2）___，社区 3___（3）___，社区 4___（4）___。除了这几种宽带接入方法以外，采用有线电视网进行宽带接入的方法是___（5）___，利用电力网进行宽带接入的方法是___（6）___，遵循 IEEE802.16 标准进行宽带接入的方法是___（7）___。

（1）～（7）备选答案：

A．FTTx+PON　　B．HFC　　C．FTTx+LAN　　D．WLAN
E．WiMax　　F．xDSL　　G. PLC（Power-Line Communication）
H．GPRS

**【问题 2】（3 分）**

在宽带接入中，FTTx 是速度最快的一种有线接入方式，而 PON（Passive Optical Network）技术是未来 FTTx 的主要解决方案。PON 目前有两种主要的技术分支，分别是 GPON 和 EPON，EPON 是___（8）___技术和___（9）___技术的结合，它可以实现上下行___（10）___的速率。

**【问题 3】（6 分）**

宽带接入通常采用 PPPoE 进行认证。PPP 协议一般包括三个协商阶段，___（11）___协议用于建立和测试数据链路；___（12）___协议用于协商网络层参数；___（13）___协议用于通信双方确认对方的身份。

**【问题 4】（4 分）**

在运营商网络中，一般会有多个用户和不同的业务流需要融合。运营商常用外层 VLAN 区分不同的___（14）___，在 ONU 或家庭网关处采用内层 VLAN 来区分不同的___（15）___；这种处理方式要求运营商网络和用户局域网中的交换机都支持___（16）___协议，同时通过 802.1ad（运营商网桥协议）来实现灵活的 QinQ 技术。

**试题一分析**

本题考查的是运营商网络接入的相关知识，属于比较新颖的题目，考查点与往年有所不同。

**【问题 1】**

本问题主要考查宽带接入网络的形式。

高速数据主干网的一个建设重点是解决“最后一公里”的问题，即宽带接入问题。

目前常见的几种宽带接入技术主要有 xDSL、FTTx+LAN、FTTx+PON、WLAN、HFC 以及 PLC 等。根据图 1-1 中的提示信息，社区 1 通过 DSLAM 以及分离器实现上网和电话同时使用，因此采用的是传统的 xdSL 技术接入网络；社区 2 通过光纤接入交换机，交换机直接连接用户，因此使用的是 FTTx+LAN 的方式接入网络；社区 3 通过 OLT 和 ONU 家庭集成网关实现上网和电话同时使用，显然采用的是 FTTx+PON 的形式；社区 4 利用无线 AP 接入网络，那么就是采用 WLAN 的方式无线接入网络。除此以外电力上网，即 PLC（ Power Line Communication），也就是利用电线实现电力线通信。它通过利用传输电流的电力线作为通信载体，使得 PLC 具有极大的便捷性。 此外，除了利用电力上网外，还可将房屋内的电话、电视、音响、冰箱等家电利用 PLC 连接起来，进行集中控制，实现“智能家庭”的梦想。HFC（Hybrid Fiber Coaxial）是光纤和同轴电缆相结合的混合网络，除可以进行有线电视信号的传输外还可以进行多媒体数据的高速传

输。Wimax，即全球微波互联接入，是一项新兴的宽带无线接入技术，遵循 IEEE 802.16 标准，特别适合户外使用。

**【问题 2】**

本问题主要考查光纤接入宽带网络系统的 PON 技术。

FTTx 技术主要应用于光纤接入宽带网络系统中，具体的应用范围包括该区域内从局端到用户端的光线路终端（Optical Line Terminal，OLT）和光网络终端（Optical Network Terminal，ONT）或光网络单元（Optical Network Unit，ONU），以及连接以上两种设备的光分配网络（Optical Distribution Network，ODN）。FTTx 的实现技术包括：点到点（P2P）和点到多点（P2MP）两种。点到多点（P2MP）技术主要应用于 PON 网络接入，常用的 FTTx 实现 PON 技术，包括 BPON（APON）、EPON、GPON。

EPON（Ethernet Passive Optical Network）以太无源光网络，由 IEEE802.3 提出定义其基本操作模式和标准，是新型光纤接入网技术之一，同时也是未来光接入网的支撑技术。EPON 综合了 PON 技术和以太网技术的优点，EPON 网络采用了 WDM 波分复用技术，以光纤作为载体，利用单根光纤实现双向速率为 1.25Gbit/s 的传输，基于 IEEE802.3ah 的 EPON 标准，规定了上下行波长（1310nm、1490nm 和 1550nm）、传输速率 1.25Gbit/s、传输距离 10/20km、最大分光比 1:64 和主要业务。

**【问题 3】**

本问题主要考查宽带接入的 PPPoE 认证原理。

PPP 是传统的认证方式之一，PPPoE 是利用以太网发送 PPP 包的传输方法和支持在同一以太网上建立多个 PPP 连接的接入技术。PPPoE 结合了以太网和 PPP 连接的综合属性。

PPP 协议是一种点到点的链路层协议，它提供了点到点的一种封装、传递数据的一种方法。PPP 协议一般包括三个协商阶段：LCP（链路控制协议）阶段，认证阶段（比如 CHAP/PAP），NCP（网络层控制协议，比如 IPCP）阶段。拨号后，用户计算机和局方的接入服务器在 LCP 阶段协商底层链路参数，然后在认证阶段通过用户计算机将用户名和密码发送给接入服务器认证，接入服务器可以进行本地认证，可以通过 RADIUS 协议将用户名和密码发送给 AAA 服务器进行认证。认证通过后，在 NCP（IPCP）协商阶段，接入服务器给用户计算机分配网络层参数如 IP 地址等。经过 PPP 的三个协商阶段后，用户就可以发送和接受网络报文。用户收发的所有网络层报文都封装在 PPP 报文中。PPP 协议的一个重要的功能提供身份验证功能。

以太网是一种广播网络，其缺点是通讯双方无法相互验证对方身份，通讯是不安全的。PPP 协议提供了通讯双方身份验证的功能，但是 PPP 协议是一种点对点的协议，协议中没有提供地址信息。如果 PPP 应用在以太网上，必须使用 PPPoE 再进行一次封装，PPPoE 协议提供了在以太网广播链路上进行点对点通讯的能力。

【问题 4】

本问题主要考查 QinQ 技术。

QinQ 技术〔也称 Stacked VLAN 或 Double VLAN〕。标准出自 IEEE 802.1ad，其实现为在 802.1q 协议标签前再次封装 802.1q 协议标签，其中一层标识用户系统网络（customer network），一层标识网络运营网络（service provider network），将其扩展实现用户线路标识，使报文带着两层 VLAN Tag 穿越运营商的骨干网络（公网）。当前部分交换机可以支持 QinQ 功能。QinQ 允许运营商为每个用户分配最大到 4K 的第二个 VLAN ID。运营商 VLAN 标记在 IPDSLAM 网络侧插入，在用户侧删除。BAS 通过识别用户的第二个 VLAN 确定用户线路标识。QinQ 也较好地解决了 VLAN（最大 4k） 数量不足问题。在实际使用中运营商常用外层 VLAN 区分不同的业务，在 ONU 或家庭网关处采用内层 VLAN 来区分不同的用户。

**参考答案**

【问题 1】

（1）F 或 xDSL

（2）C 或 FTTx+LAN

（3）A 或 FTTx+PON

（4）D 或 WLAN

（5）B 或 HFC

（6）G 或 PLC（Power-Line Communication）

（7）E 或 WiMax

【问题 2】

（8）以太网

（9）PON （注：（8）（9）可互换）

（10）1.25Gbps

【问题 3】

（11）LCP（链路控制协议）

（12）NCP（网络层控制协议）

（13）认证（CHAP/PAP）

【问题 4】

（14）业务

（15）用户

（16）802.1Q

**试题二（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

为了保障网络安全，某公司安装了一款防火墙，对内部网络、Web 服务器以及外部

网络进行逻辑隔离，其网络结构如图 2-1 所示。

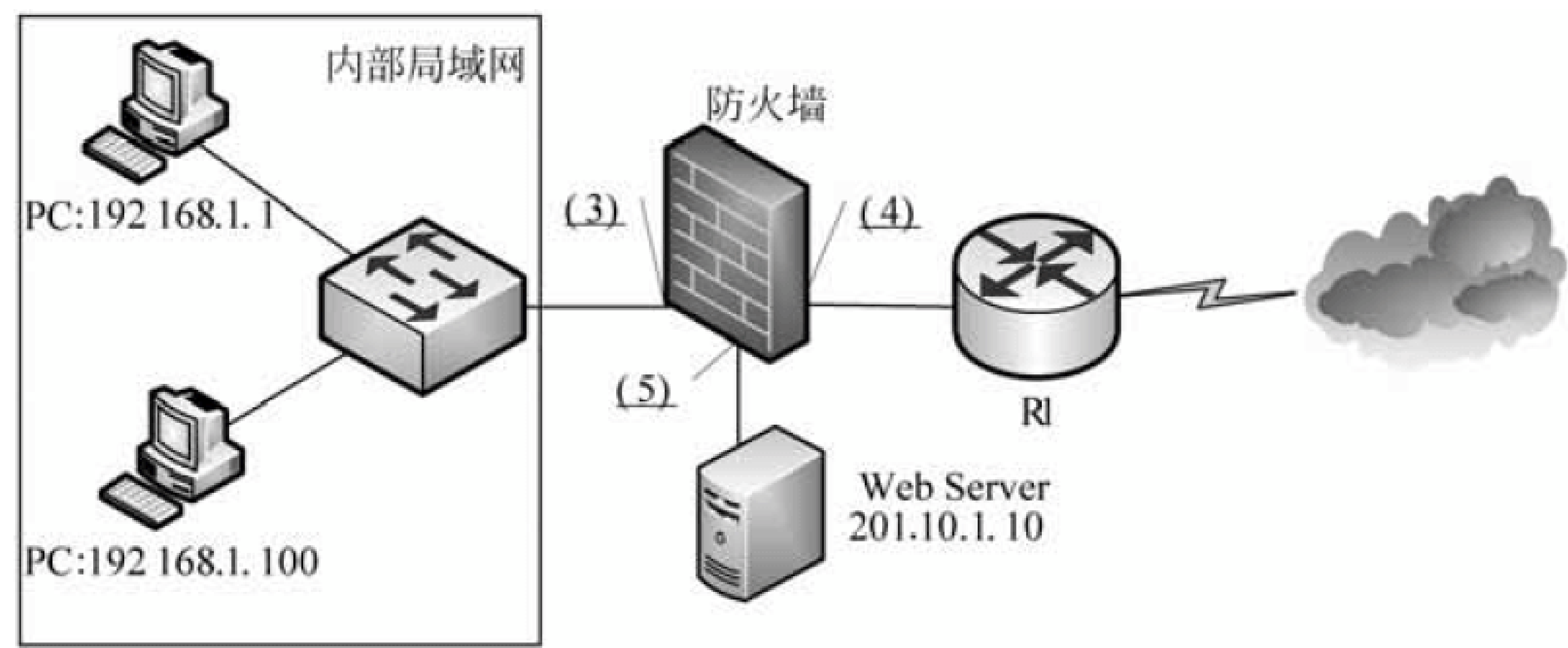



图 2-1

【问题 1】(4 分)

包过滤防火墙使用 ACL 实现过滤功能，常用的 ACL 分为两种，编号为 1-99 的 ACL 根据 IP 报文的源地址域进行过滤，称为__(1)__；编号为 100-199 的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为__(2)__。

【问题 2】(3 分)

根据图 2-1，防火墙的三个端口连接的网络分别称为__(3)__、__(4)__和__(5)__。

【问题 3】(7 分)

防火墙配置要求如下：

- 公司内部局域网用户可以访问 Web Server 和 Internet；
- Internet 用户可以访问 Web Server；
- Internet 上特定主机 202.110.1.100 可以通过 Telnet 访问 Web Server；
- Internet 用户不能访问公司内部局域网。

请按照防火墙的最小特权原则补充完成表 2-1。

**表 2-1**

| 源 地 址 | 源 端 口 | 目 的 地 址 | 目 的 端 口 | 协 议 | 规 则 |
|---|---|---|---|---|---|
| Any | Any | (6) | (7) | WWW | 允许 |
| 192.168.1.0/24 | Any | (8) | (9) | Any | 允许 |
| 202.110.1.100 | Any | (10) | (11) | TELNET | 允许 |
| Any | Any | Any | Any | Any | (12) |

【问题 4】(6 分)

由于防火墙出现故障，现将网络拓扑进行调整，增加一台包过滤路由器 R2，与 Proxy Server 和路由器 R1 共同组成一个屏蔽子网防火墙，结构如图 2-2 所示。为了实现与表 2-1 相同的过滤功能，补充路由器 R1 上的 ACL 规则。

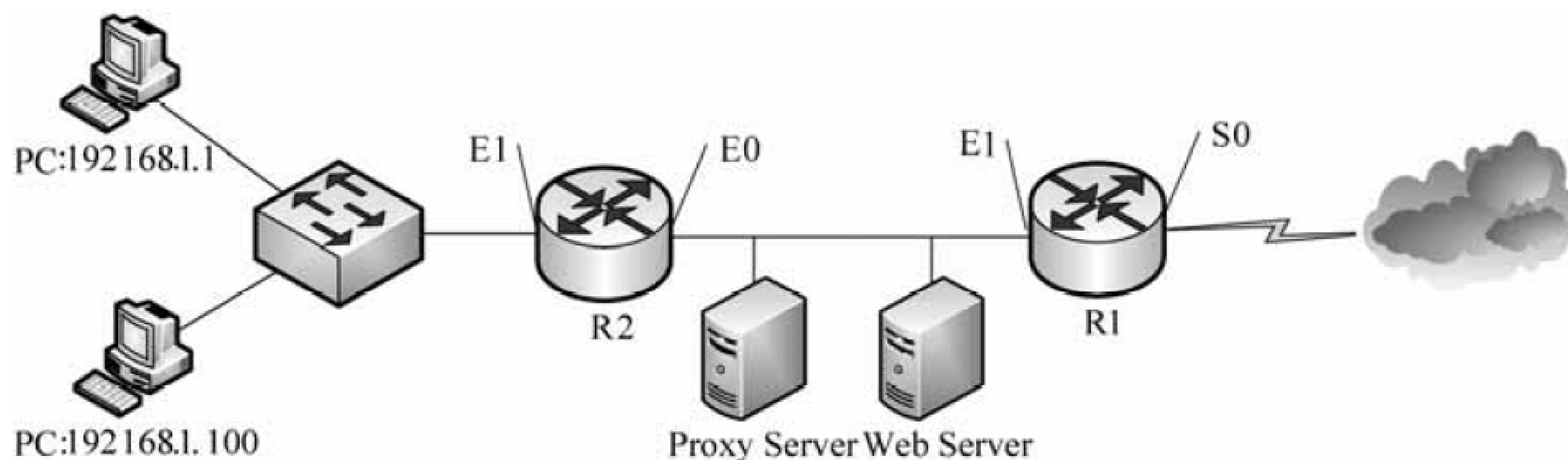



图 2-2

```
R1>…
R1(config-s0)> access-list 101 permit  (13)
  //允许 Internet 用户访问 WebServer
R1(config-s0)> access-list 101 permit (14)
  //允许主机 202.110.1.100 Telnet 到 Web Server
R1(config-s0)> access-list 101  (15)
  //禁止所有 IP 包
R1 (config-s0)> ip access-group 101 in
  //应用 101 规则到 s0 入口

R1>…
R1(config-ethernet1)> access-list 102 permit ip any any
R1 (config-ethernet1)> ip access-group 102 out
R1>…
```

## 试题二分析

本题考查网络安全中包过滤功能及 ACL 的语法与应用。

**【问题 1】**

包过滤防火墙使用 ACL 实现过滤功能，常用的 ACL 分为两种，编号为 1-99 的 ACL 根据 IP 报文的源地址域进行过滤，称为标准访问控制列表（标准 ACL）；编号为 100-199 的 ACL 根据 IP 报文中的更多域对数据包进行控制，称为扩展访问控制列表（扩展 ACL）。

**【问题 2】**

防火墙的端口连接的网络依据被保护对象的安全级别分为三个：内网（Trusted）有要保护的数据和主机，安全级别最高；DMZ（非军事区）放置可对外提供的服务器群，安全级别次之；外网（Untrusted）是内网用户可访问资源，安全设置较少，安全级别最低。

**【问题 3】**

表中第一条规则允许 WWW 服务，对应要求中的第 2 条，即 Internet 用户可以访问 Web Server，故目的地址及目的端口分别是服务器的 IP 地址和 80 端口号；

第二条规则源地址为 192.168.1.0/24，对应要求中的第 1 条，即公司内部局域网用户可以访问 Web Server 和 Internet，故目的地址和端口号为任意值均可，故（8）、（9）处应填 any 和 any；

第三条规则源地址为 202.110.1.100、服务为 TELNET，对应要求中的第 3 条，即 Internet 上特定主机 202.110.1.100 可以通过 Telnet 访问 Web Server，故目的地址和端口号为服务器的 IP 地址和 TELNET 的端口号 23；

第四条规则对应要求中的第 4 条，即 Internet 用户不能访问公司内部局域网，故规则动作为拒绝。

**【问题 4】**

空（13）处为允许 Internet 用户访问 WebServer，故语句为：tcp any host 201.10.1.10 eq www

空（14）处为允许主机 202.110.1.100 Telnet 到 Web Server，故语句为：tcp host 202.110.1.100 host 201.10.1.10 eq telnet

空（15）处为禁止所有 IP 包，故语句为：deny ip any any

**参考答案**

**【问题 1】**

（1）标准访问控制列表（标准 ACL）（2）扩展访问控制列表（扩展 ACL）

**【问题 2】**

（3）内网（Trusted）　（4）外网（Untrusted）　（5）DMZ（非军事区）

**【问题 3】**

（6）201.10.1.10　（7）80　（8）Any　（9）Any

（10）201.10.1.10　（11）23　（12）拒绝

**【问题 4】**

（13）tcp any host 201.10.1.10 eq www

（14）tcp host 202.110.1.100 host 201.10.1.10 eq telnet

（15）deny ip any any

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 7，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位网络拓扑结构如图 3-1 所示，内部各计算机终端通过代理服务器访问 Internet，网络要求如下：

1. 运营商提供的 IP 地址为 202.117.112.0/30，网络出口对端 IP 地址为 202.117.112.1；
2. 代理服务器采用 Linux 系统；
3. Web、DNS 和 DHCP 服务器采用 Windows Server 2003 系统，Web 服务器 IP 地

址为 192.168.0.3，DNS 服务器 IP 地址为 192.168.0.2，DHCP 服务器 IP 地址为 192.168.0.4；

4．内部客户机采用 Windows XP 系统，通过 DHCP 服务器动态分配 IP 地址，子网为 192.168.0.0/25，内网网关 IP 地址为 192.168.0.1；

5．代理服务器、DNS、Web 和 DHCP 服务器均通过手动设置 IP 地址。

**【问题 1】（2 分）**

Linux 系统中，IP 地址的配置文件一般存放在__（1）__目录下。

A. /etc　　B. /var　　C. /dev　　D. /home

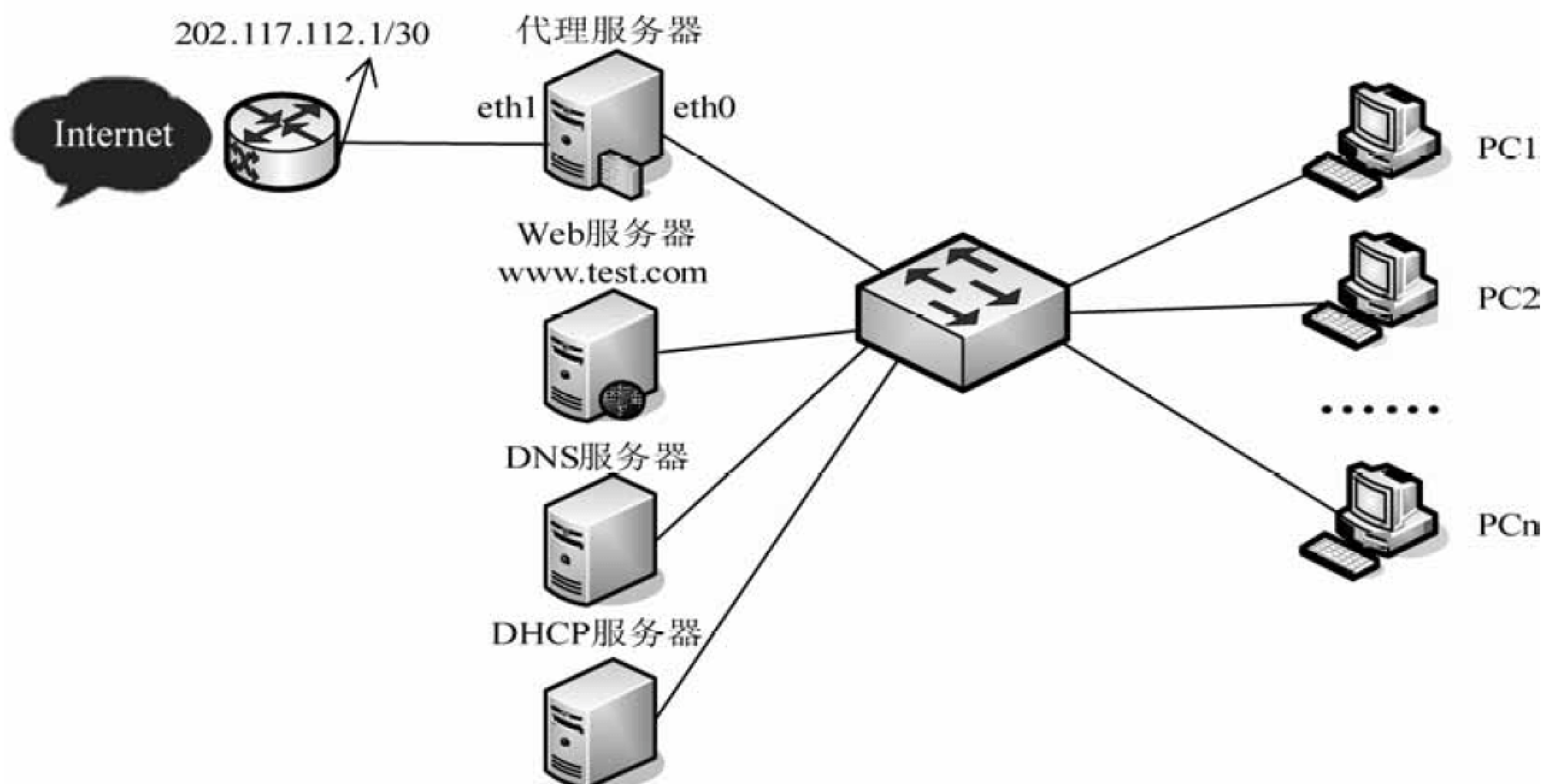



图 3-1

**【问题 2】（3 分）**

请完成图 3-1 中代理服务器 eth0 的配置。

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK=__(2)__
IPADDR=__(3)__
GATEWAY=192.168.0.1
TYPE=Ethernet
NAME="ystem eth0"
IPV6INIT=no
```

**【问题 3】（3 分）**

请完成图 3-1 中代理服务器 eth1 的配置。

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK= (4)
IPADDR= (5)
GATEWAY= (6)
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
DEVICE=eth0
```

**【问题 4】（4 分）**

DNS 使用__（7）__来处理网络中多个主机和 IP 地址的转换，当 DNS 服务器配置完成后，在客户机的 cmd 命令窗口中，可用于测试 DNS 服务状态的命令有__（8）__（多选）。

（7）备选答案：

A．集中式数据库　　　　B．分布式数据库

（8）备选答案：

A．nslookup　　B．arp　　C．ping　　D．tracert

E．ipconfig

**【问题 5】（2 分）**

安装 DNS 服务时，在图 3-2 所示 Windows 组件中，选择__（9）__，然后点击“详细信息”进行 DNS 组件安装。

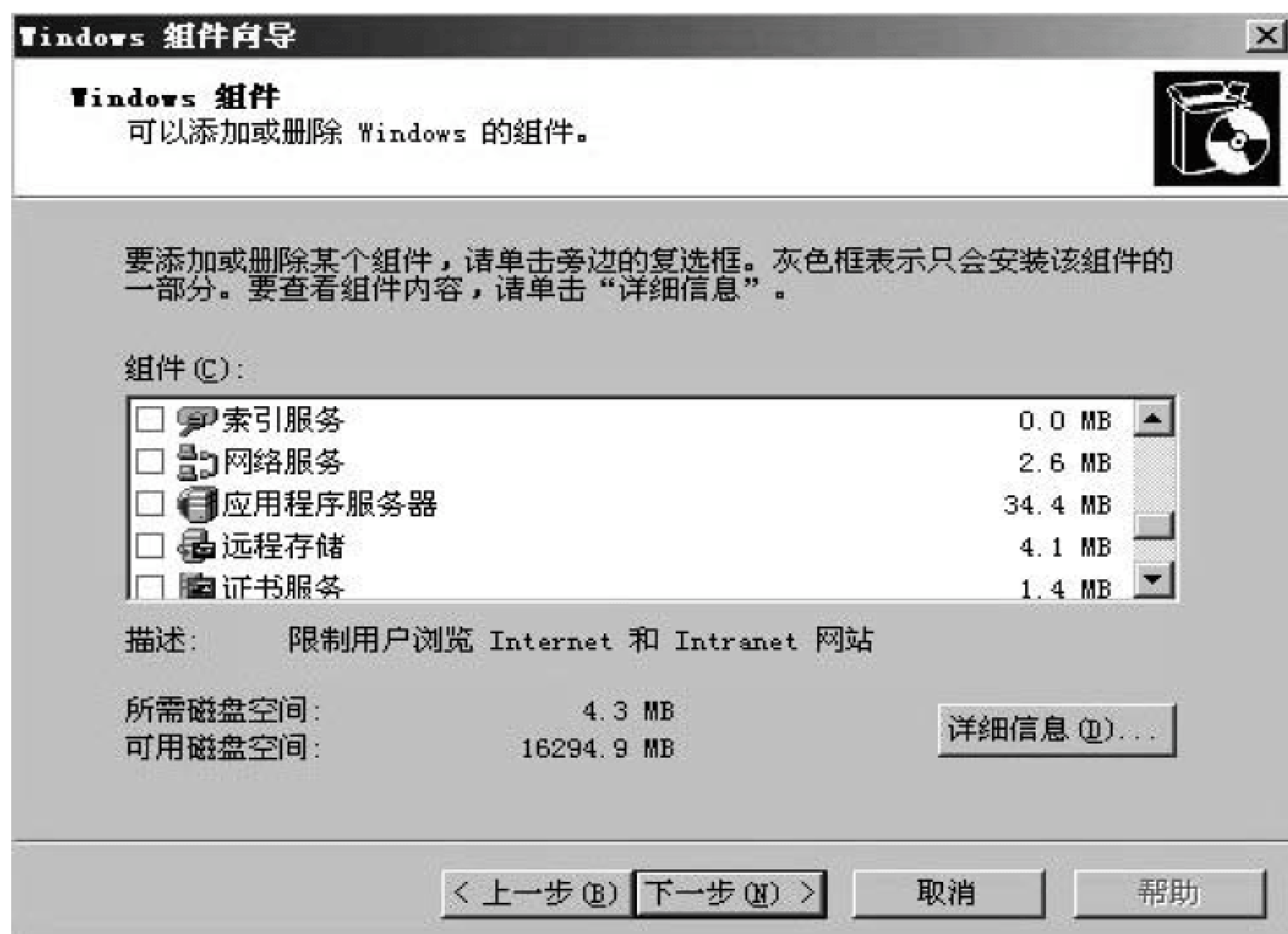



图 3-2

**【问题 6】（3 分）**

在 DNS 服务器中为 Web 服务器添加主机记录时，在图 3-3 中区域名称应填写<u>（10）</u>来建立正向查找区域。在图 3-4 所示的“新建主机”对话框中名称栏应填写<u>（11）</u>，IP 地址栏应填写<u>（12）</u>。

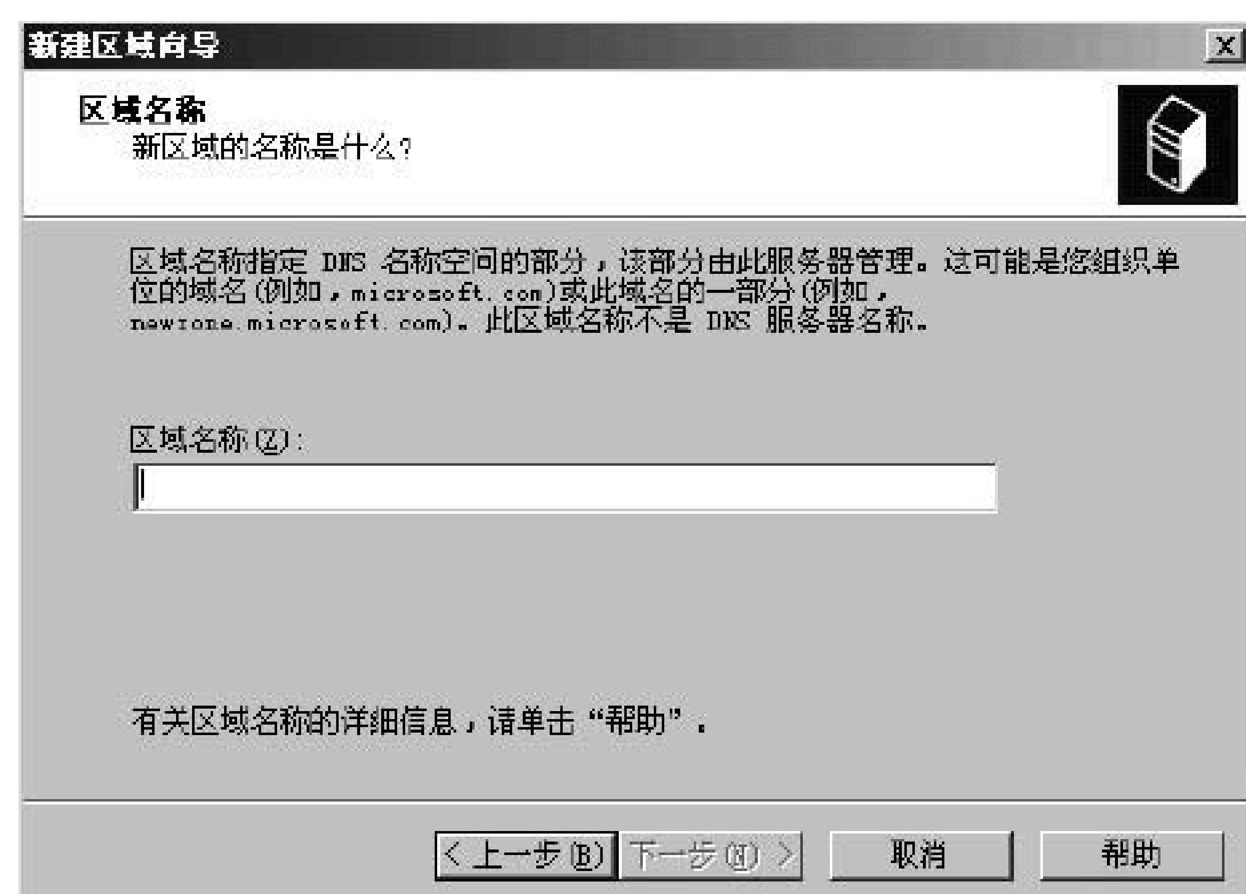



图 3-3

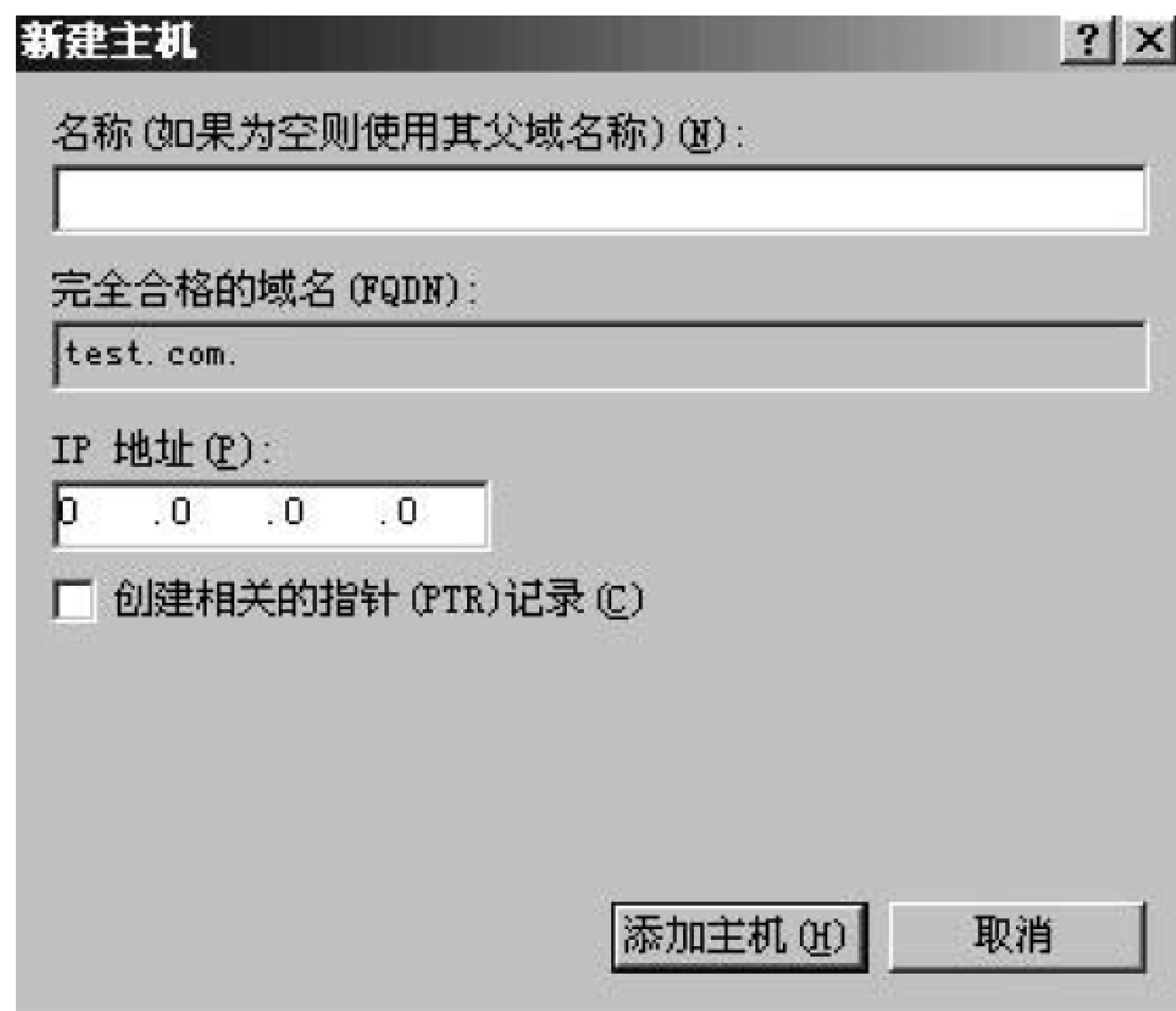



图 3-4

**【问题 7】（3 分）**

在建立反向区域时，图 3-5 中的“网络 ID”中输入<u>（13）</u>。在图 3-6 所示的创建指针记录对话框中，主机的 IP 地址为<u>（14）</u>，主机名为<u>（15）</u>。

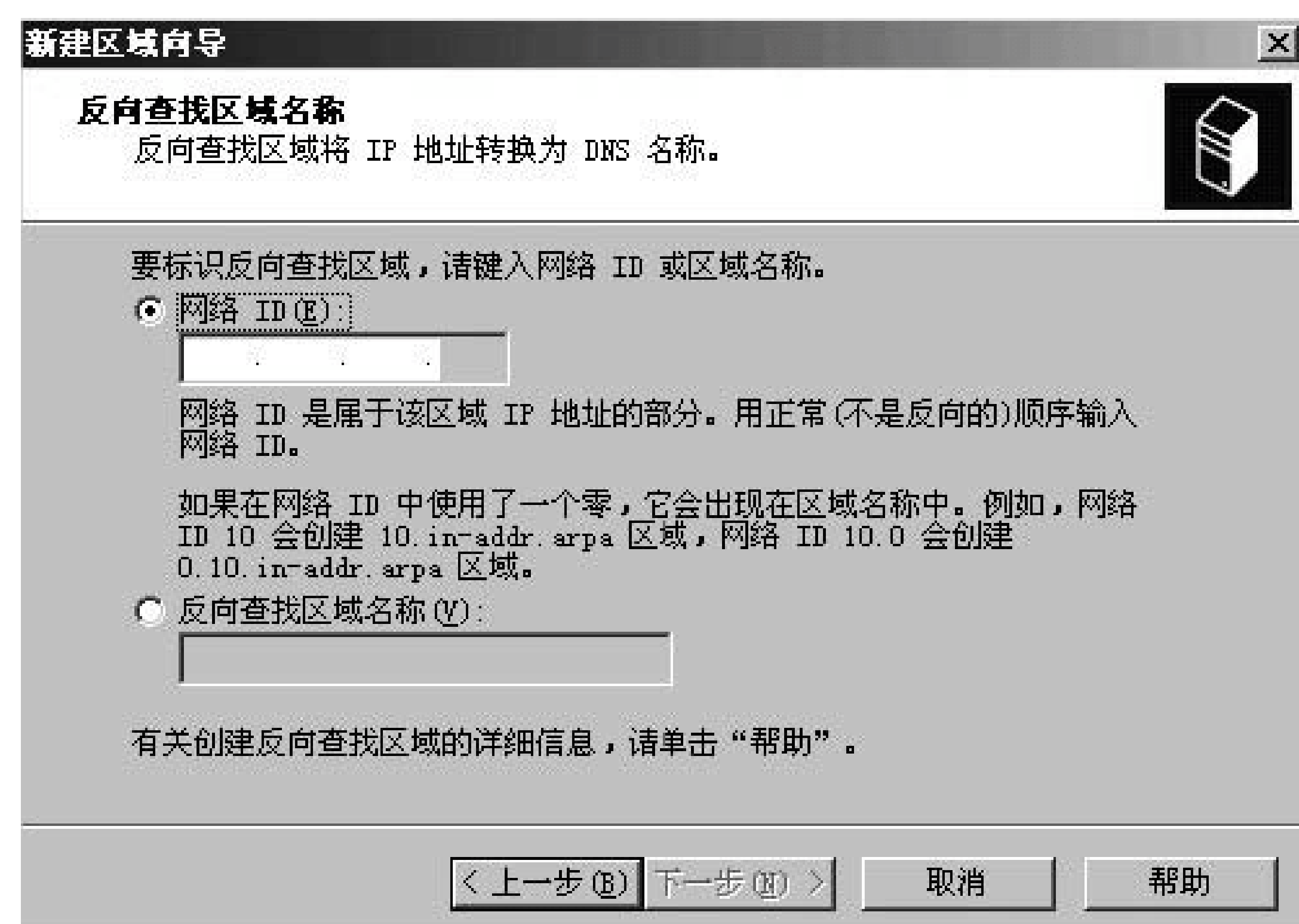



图 3-5




图 3-6

**试题三分析**

本题考查考生在 Linux 操作系统中 TCP/IP 的配置和 Windows 操作系统中 DNS 服务器配置的相关知识。

**【问题 1】**

本问题主要考查考生对 Linux 操作系统中目录的了解程度。

Linux 系统中，IP 地址的配置文件一般存放在/etc 目录下。

**【问题 2】**

本问题主要考查对文本方式下网络配置的掌握程度。

HWADDR 是 MAC 地址信息，NETMASK 是网络掩码信息，IPADDR 是 IP 地址，GATEWAY 为网关 IP 地址。

**【问题 3】**

本问题主要考查对文本方式下网络配置的掌握程度。

HWADDR 是 MAC 地址信息，NETMASK 是网络掩码信息，IPADDR 是 IP 地址，GATEWAY 为网关 IP 地址。

**【问题 4】**

本问题主要考查 DNS 原理和测试命令。

nslookup 命令是一个用于查询 Internet域名信息或诊断 DNS 服务器问题的工具。

arp 命令可用于查询本机 ARP 缓存、添加或删除静态对应关系。

ping 命令是因特网包探索器，用于测试网络连接量的程序，当 ping 域名时可以根据能否返回 IP 地址来判断 DNS 状态。

tracert 命令是路由跟踪实用程序，可以通过追踪域名查看能否返回相应 IP 地址来判断 DNS 状态。

ipconfig 命令是调试计算机网络的常用命令。

**【问题 5】**

DNS 组件属于网络服务组件。

**【问题 6】**

本问题主要考查考生对 Windows Server 2003 操作系统中具体添加正向解析记录操作的掌握程度。

在添加主机记录时，为区域名为 test.com、名称栏为 www 来建立正向查找区域，对应的 IP 地址为 192.168.0.3。

**【问题 7】**

本问题主要考查考生对 Windows Server 2003 操作系统中具体添加反向解析记录操作的掌握程度。

在建立反向区域时，网络 ID 应为 192.168.0.0。在创建指针记录对话框中，主机的 IP 地址为 192.168.0.3，主机名为 www. test.com。

## 参考答案

**【问题 1】**

（1）A 或 /etc

**【问题 2】**

（2）255.255.255.128　（3）192.168.0.1

**【问题 3】**

（4）255.255.255.252　（5）202.117.112.2　（6）202.117.112.1

**【问题 4】**

（7）B 或 分布式数据库　（8）A 、C、D 或 nslookup、ping、tracert

**【问题 5】**

（9）网络服务

**【问题 6】**

（10）test.com　（11）www　（12）192.168.0.3

**【问题 7】**

（13）192.168.0.0　（14）3　（15）www.test.com

## 试题四（共 15 分）

阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司计划使用路由器作为 DHCP Server，其网络拓扑结构如图 4-1 所示。根据业务需求，公司服务器 IP 地址使用 192.168.2.1/24，部门 1 使用 192.168.4.1/24 网段、部门 2 使用 192.168.3.1/24 网段（其中 192.168.3.1～192.168.3.10 地址保留不分配），部门 1 和部门 2 通过路由器的 DHCP 服务自动获取 IP 地址。

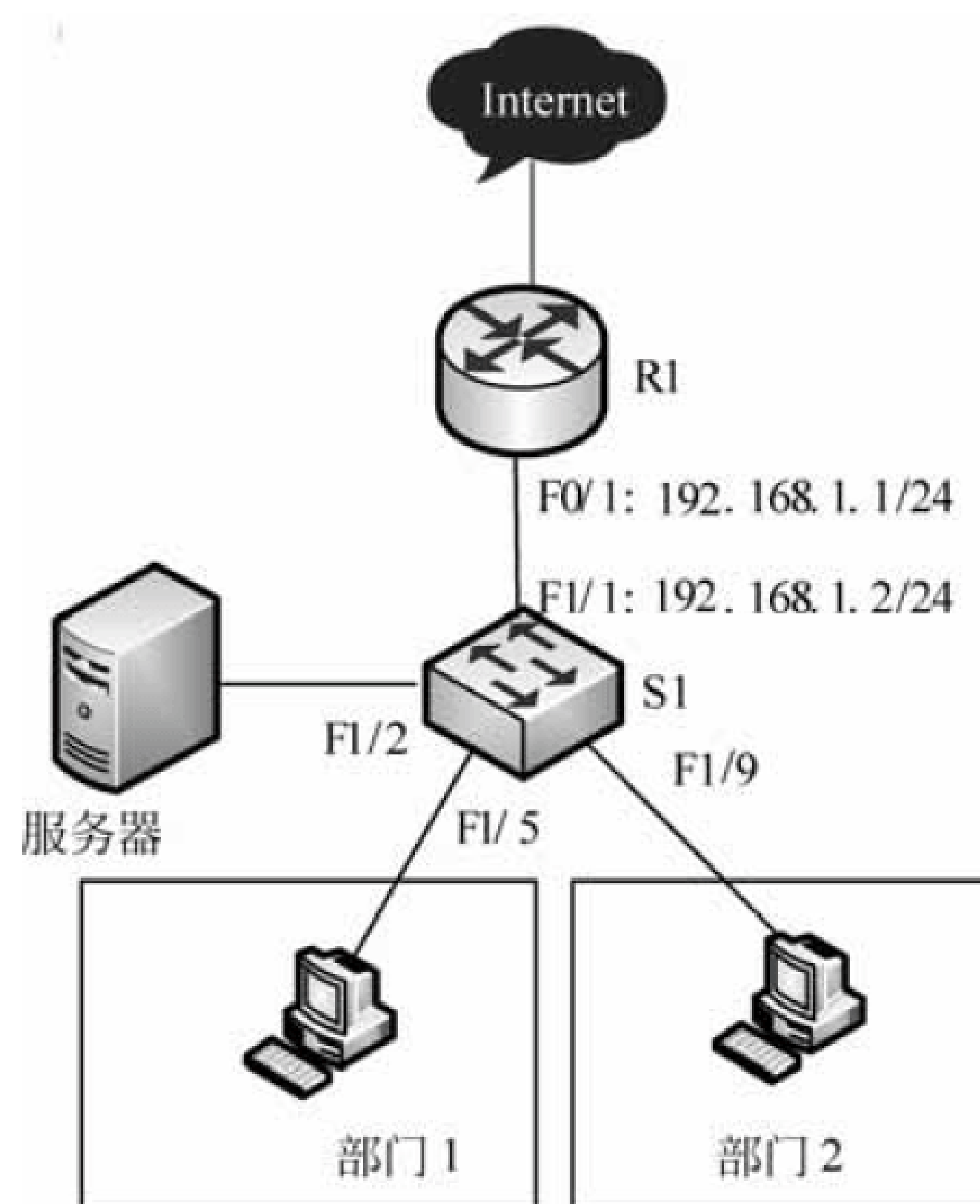



图 4-1

**【问题 1】（10 分）**

根据网络拓扑和需求说明，完成（或解释）路由器 R1 的配置：

```
R1#config t
R1 (config)# interface FastEthernet0/1
R1 (config-if)#ip address  (1)  (2)
R1 (config-if)#no shutdown
R1(config-if)#exit
R1 (config)#ip dhcp pool vlan 3
R1 (dhcp-config)# network 192.168.3.0 255.255.255.0
R1 (dhcp-config)# default-router  192.168.3.254 255.255.255.0
                                                    ;  (3)
R1 (dhcp-config)# dns-server 192.168.2.1            ;  (4)
R1 (dhcp-config)# lease 0 8 0                       ;  (5)
R1 (dhcp-config)#exit
R1 (config)# ip dhcp pool vlan 4
R1(dhcp-config)# network  (6)  (7)
R1 (dhcp-config)# default-router  192.168.4.254 255.255.255.0
R1 (dhcp-config)# dns-server 192.168.2.1
R1 (dhcp-config)# lease 0 8 0
R1 (dhcp-config)#exit
R1 (config)# ip dhcp excluded-address  (8)  (9)
R1 (config)# ip dhcp excluded-address 192.168.3.254     ;排除掉不能分配的IP地址
R1 (config)# ip dhcp excluded-address 192.168.4.254

R1 (config)# (10)  192.168.3.0 255.255.255.0 FastEthernet0/1  ;在以太网接口和VLAN3间建立一条静态路由
......
```

**【问题 2】（5 分）**

根据网络拓扑和需求说明，完成（或解释）交换机 S1 的部分配置。

```
S1#config t
S1(config)#interface vlan2
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan3
S1(config-if)# ip helper-address  (11)        ;指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan4
......
S1(config)#interface f1/1
```

```
S1(config-if)#switchport mode  (12)
S1(config-if)# switchport trunk allowed vlan all
S1(config-if)#exit
S1(config)#interface f1/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access  (13)
S1(config-if)#exit
S1(config)#interface f1/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access  (14)
S1(config)#interface f1/9
S1(config-if)#switchport mode access
S1(config-if)#switchport access  (15)
......
```

**试题四分析**

本题考查交换机及路由器的基本配置。

**【问题 1】**

本问题考查路由器的接口配置及 DHCP 服务设置。

根据图 4-1 可以确定路由器的接口地址及 vlan4 的地址范围，同时题目说明明确指出了 192.168.3.1～192.168.3.10 地址保留不分配。所以路由器的配置及说明应如下所示：

```
R1#config t
R1 (config)# interface FastEthernet0/1
R1 (config-if)#ip address 192.168.1.1 255.255.255.0

R1 (config-if)#no shutdown
R1(config-if)#exit
R1 (config)#ip dhcp pool vlan 3
R1 (dhcp-config)# network 192.168.3.0 255.255.255.0
R1 (dhcp-config)# default-router  192.168.3.254 255.255.255.0 ;设 vlan3
默认网关及掩码
R1 (dhcp-config)# dns-server 192.168.2.1        ;设 dns 服务器地址
R1 (dhcp-config)# lease 0 8 0                   ;设 dhcp 租约为 8 小时
R1 (dhcp-config)#exit
R1 (config)# ip dhcp pool vlan 4
R1(dhcp-config)# network 192.168.4.0  255.255.255.0
R1 (dhcp-config)# default-router  192.168.4.254 255.255.255.0
R1 (dhcp-config)# dns-server 192.168.2.1
R1 (dhcp-config)# lease 0 8 0
R1 (dhcp-config)#exit
```

```
R1 (config)# ip dhcp excluded-address 192.168.3.1  192.168.3.10
R1 (config)# ip dhcp excluded-address 192.168.3.254
                                          ;排除掉不能分配的 IP 地址
R1 (config)# ip dhcp excluded-address 192.168.4.254

R1 (config)# ip route 192.168.3.0 255.255.255.0 FastEthernet0/1
                              ;在以太网接口和 VLAN3 间建立一条静态路由
……
```

**【问题 2】**

本问题考查交换机基本配置。依据问题 1 可以确定 DHCP 服务器的地址，根据拓扑图可以判定交换机各个接口连接的部门，再根据题目描述确定其 Vlan，所以该交换机的配置如下：

```
S1#config t
S1(config)#interface vlan2
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan3
S1(config-if)# ip helper-address  192.168.1.1   ;指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan4
……
S1(config)#interface f1/1
S1(config-if)#switchport mode trunk
S1(config-if)# switchport trunk allowed vlan all
S1(config-if)#exit
S1(config)#interface f1/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan2
S1(config-if)#exit
S1(config)#interface f1/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan4
S1(config)#interface f1/9
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan3
```

## 参考答案

**【问题 1】**

（1）192.168.1.1

（2）255.255.255.0

（3）设置 vlan3 默认网关及掩码

（4）设置 dns 服务器地址

（5）设置 dhcp 租约时间为 8 小时

（6）192.168.4.0

（7）255.255.255.0

（8）192.168.3.1

（9）192.168.3.10

（10）ip route

**【问题 2】**

（11）192.168.1.1

（12）trunk

（13）vlan2

（14）vlan4

（15）vlan3

# 第 21 章　2014 上半年网络工程师上午试题分析与解答

**试题（1）**

在 CPU 中，常用来为 ALU 执行算术逻辑运算提供数据并暂存运算结果的寄存器是 __(1)__。

（1）A．程序计数器　　B．状态寄存器

　　C．通用寄存器　　D．累加寄存器

**试题（1）分析**

本题考查计算机系统基础知识。

CPU 中有一些重要的寄存器，程序计数器（PC）用于存放指令的地址。当程序顺序执行时，每取出一条指令，PC 内容自动增加一个值，指向下一条要取的指令。当程序出现转移时，则将转移地址送入 PC，然后由 PC 指出新的指令地址。

状态寄存器用于记录运算中产生的标志信息。状态寄存器中的每一位单独使用，称为标志位。标志位的取值反映了 ALU 当前的工作状态，可以作为条件转移指令的转移条件。典型的标志位有以下几种：进位标志位（C）、零标志位（Z）、符号标志位（S）、溢出标志位（V）、奇偶标志位（P）。

通用寄存器组是 CPU 中的一组工作寄存器，运算时用于暂存操作数或地址。在程序中使用通用寄存器可以减少访问内存的次数，提高运算速度。累加器（accumulator）：累加器是一个数据寄存器，在运算过程中暂时存放操作数和中间运算结果，不能用于长时间地保存一个数据。

**参考答案**

（1）D

**试题（2）**

某机器字长为 n，最高位是符号位，其定点整数的最大值为 __（2）__。

（2）A．$2^n-1$　　B．$2^{n-1}-1$　　C．$2^n$　　D．$2^{n-1}$

**试题（2）分析**

本题考查计算机系统中数据表示基础知识。

机器字长为 $n$，最高位为符号位，则剩余的 $n-1$ 位用来表示数值，其最大值是这 $n-1$ 位都为 1，也就是 $2^{n-1}-1$。

**参考答案**

（2）B

**试题（3）、（4）**

通常可以将计算机系统中执行一条指令的过程分为取指令、分析和执行指令 3 步，若取指令时间为 4Δ*t*，分析时间为 2Δ*t*，执行时间为 3Δ*t*，按顺序方式从头到尾执行完 600 条指令所需时间为__（3）__Δ*t*；若按照执行第 i 条、分析第 i+1 条、读取第 i+2 条重叠的流水线方式执行指令，则从头到尾执行完 600 条指令所需时间为__（4）__Δt。

（3）A．2400　　B．3000　　C．3600　　D．5400

（4）A．2400　　B．2405　　C．3000　　D．3009

**试题（3）、（4）分析**

本题考查指令系统基础知识。

指令顺序执行时，每条指令需要 9Δ*t*(4Δ*t*＋2Δ*t*＋3Δ*t*)，执行完 600 条指令需要 5400Δ*t*，若采用流水方式，则在分析和执行第 1 条指令时，就可以读取第 2 条指令，当第 1 条指令执行完成，第 2 条指令进行分析和执行，而第 3 条指令可进行读取操作。因此，第 1 条指令执行完成后，每 4Δ*t* 就可以完成 1 条指令，600 条指令的总执行时间为 9Δ*t*＋599×4Δ*t* =2405Δ*t*。

**参考答案**

（3）D　　（4）B

**试题（5）**

若用 256k×8bit 的存储器芯片，构成地址 40000000H 到 400FFFFFH 且按字节编址的内存区域，则需__（5）__片芯片。

（5）A．4　　B．8　　C．16　　D．32

**试题（5）分析**

本题考查计算机系统中存储器知识。

地址 400000000H 到 4000FFFFFH 共有 FFFFFH（即 $2^{20}$）个以字节为单位的编址单元，而 256k×8bit 的存储器芯片可提供 $2^{18}$ 个以字节为单位的编址单元，因此需要 4 片（$2^{20}/2^{18}$）这种芯片来构成上述内存区域。

**参考答案**

（5）A

**试题（6）**

以下关于进度管理工具 Gantt 图的叙述中，不正确的是__（6）__。

（6）A．能清晰地表达每个任务的开始时间、结束时间和持续时间

B．能清晰地表达任务之间的并行关系

C．不能清晰地确定任务之间的依赖关系

D．能清晰地确定影响进度的关键任务

**试题（6）分析**

本题考查软件项目管理的基础知识。

Gantt 图是一种简单的水平条形图，以日历为基准描述项目任务。水平轴表示日历时间线，如天、周和月等，每个条形表示一个任务，任务名称垂直的列在左边的列中，图中水平条的起点和终点对应水平轴上的时间，分别表示该任务的开始时间和结束时间，水平条的长度表示完成该任务所持续的时间。当日历中同一时段存在多个水平条时，表示任务之间的并发。

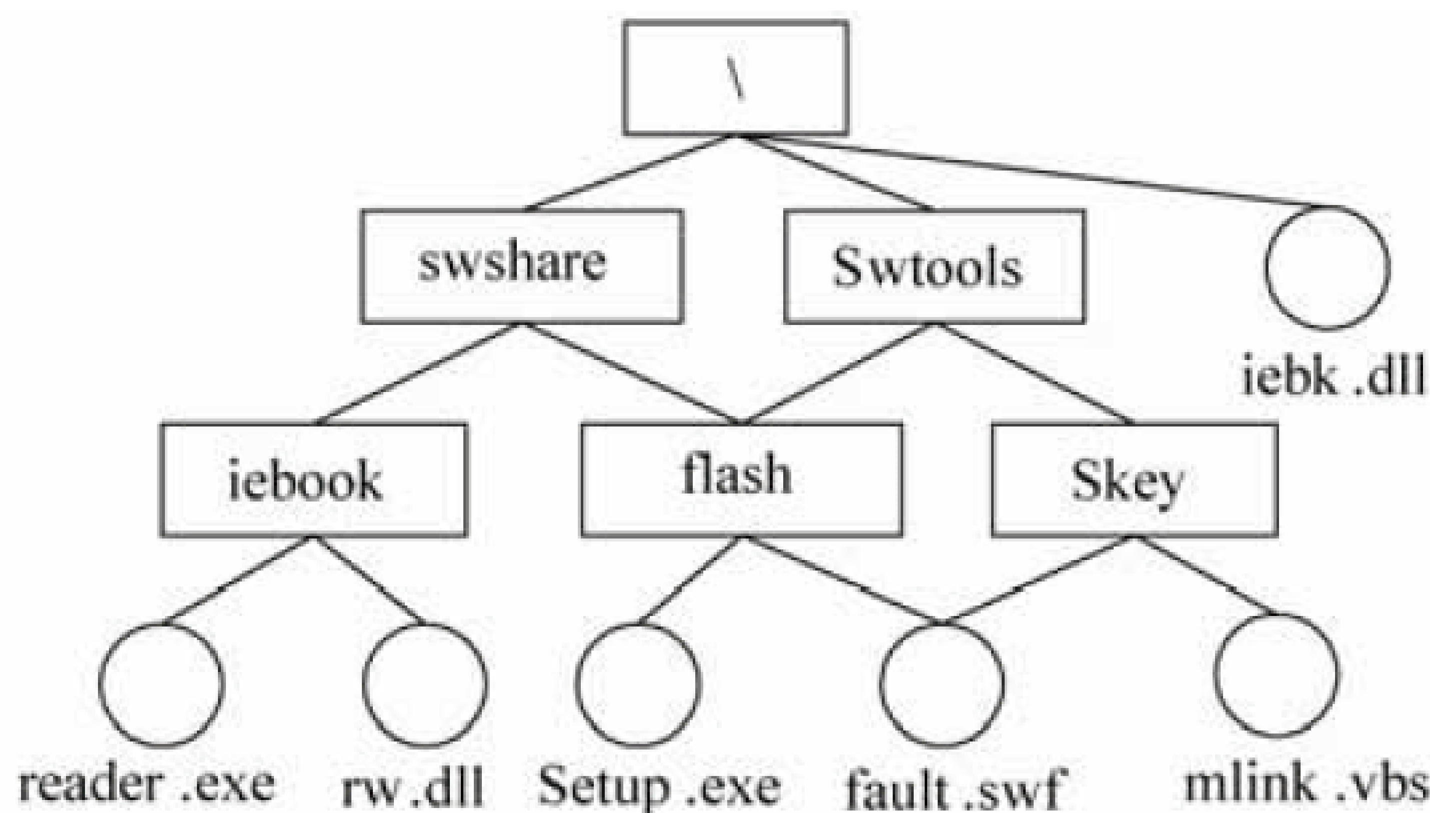
Gantt 图能清晰地描述每个任务从何时开始，到何时结束，任务的进展情况以及各个任务之间的并行性。但它不能清晰地反映出各任务之间的依赖关系，难以确定整个项目的关键所在，也不能反映计划中有潜力的部分。

**参考答案**

（6）D

**试题（7）、（8）**

若某文件系统的目录结构如下图所示，假设用户要访问文件 fault.swf，且当前工作目录为 swshare，则该文件的全文件名为__（7）__，相对路径和绝对路径分别为__（8）__。




（7）A．fault.swf　　B．flash\fault.swf
　　C．swshare\flash\fault.swf　　D．\swshare\flash\fault.swf

（8）A．swshare\flash\和\flash\　　B．flash\和\swshare\flash\
　　C．\swshare\flash\和 flash\　　D．\flash\和\swshare\flash\

**试题（7）、（8）分析**

本题考查对操作系统文件管理方面的基础知识。

路径名是指操作系统查找文件所经过的目录名以及目录名之间的分隔符构成的。通常，操作系统中全文件名是指路径名+文件名。

按查找文件的起点不同可以将路径分为：绝对路径和相对路径。从根目录开始的路径称为绝对路径；从用户当前工作目录开始的路径称为相对路径，相对路径是随着当前工作目录的变化而改变的。

**参考答案**

（7）D　　（8）B

**试题（9）**

在引用调用方式下进行函数调用，是将__（9）__。

（9）A. 实参的值传递给形参　　B. 实参的地址传递给形参
C. 形参的值传递给实参　　D. 形参的地址传递给实参

**试题（9）分析**

本题考查程序语言基础知识。

值调用和引用调用是实现函数调用时传递参数的两种基本方式。在值调用方式下，是将实参的值传给形参，在引用调用方式下，实将实参的地址传递给形参。

**参考答案**

（9）B

**试题（10）**

王某买了一幅美术作品原件，则他享有该美术作品的__（10）__。

（10）A. 著作权　　B. 所有权
C. 展览权　　D. 所有权与其展览权

**试题（10）分析**

本题考查知识产权基本知识。

绘画、书法、雕塑等美术作品的原件可以买卖、赠予。但获得一件美术作品并不意味着获得该作品的著作权。我国著作权法规定："美术等作品原件所有权的转移，不视为作品著作权的转移，但美术作品原件的展览权由原件所有人享有。"这就是说作品物转移的事实并不引起作品著作权的转移，受让人只是取得物的所有权和作品原件的展览权，作品的著作权仍然由作者享有。

**参考答案**

（10）D

**试题（11）、（12）**

路由器连接帧中继网络的接口是__（11）__，连接双绞线以太网的接口是__（12）__。

（11）A. AUI 接口　B. RJ-45 接口　C. Console 接口　D. Serial 接口
（12）A. AUI 接口　B. RJ-45 接口　C. Console 接口　D. Serial 接口

**试题（11）、（12）分析**

路由器有以下几种联网接口：

① RJ-45 端口：在这种端口上通过双绞线连接以太网。10Base-T 的 RJ-45 端口标识为"ETH"，而 100Base-TX 的 RJ-45 端口标识为"10/100bTX"，这是因为快速以太网路由器采用 10/100Mb/s 自适应电路。

② AUI 端口：这是一种 D 型 15 针连接器，用在令牌环网或总线型以太网中。路由器经 AUI 端口通过粗同轴电缆收发器连接 10Base-5 网络，也可以通过外接的 AUI-to-RJ-45 适配器连接 10Base-T 以太网，还可以借助其他类型的适配器实现与

10Base-2 细同轴电缆或 10Base-F 光缆的连接。

③ 高速同步串口：在路由器与广域网的连接中，应用最多的是高速同步串行口（Synchronous Serial Port），这种端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。通过这种端口所连接的网络两端要求同步通信，以很高的速率进行数据传输。

④ ISDN BRI 端口：这种端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 三个通道（2B+D）的总带宽为 144 kb/s，端口采用 RJ-45 标准，与 ISDN NT1 的连接使用 RJ-45-to-RJ-45 直通线。

⑤ Console 端口：Console 端口通过配置专用电缆连接至计算机串行口，利用终端仿真程序（如 Windows 中的超级终端）对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。Console 端口不支持硬件流控。

⑥ AUX 端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Prot）。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行电路转换。AUX 端口支持硬件流控。

⑦ 异步串口：异步串口（ASYNC）主要应用于与 Modem 或 Modem 池的连接，以实现远程计算机通过 PSTN 拨号接入。异步端口的速率不是很高，也不要求同步传输，只要求能连续通信就可以了。

**参考答案**

（11）D　（12）B

**试题（13）**

在地面上相距 2000 公里的两地之间通过电缆传输 4000 比特长的数据包，数据速率为 64Kb/s，从开始发送到接收完成需要的时间为__（13）__。

（13）A．48ms　B．640ms　C．32.5ms　D．72.5ms

**试题（13）分析**

从开始发送到接收完成的时间包含数据包的发送（或接收）时间，以及信号在电缆中的传播延迟时间。电信号在电缆中的传播速度是 200m/μs，所以传播延迟时间为 2000Km÷200m/μs＝10ms，而发送（或接收）数据包的时间为 4000bit÷64Kb/s＝62.5ms，总共是 72.5ms。

**参考答案**

（13）D

**试题（14）、（15）**

海明码是一种纠错编码，一对有效码字之间的海明距离是__（14）__。如果信息为 6 位，要求纠正 1 位错，按照海明编码规则，需要增加的校验位是__（15）__位。

（14）A．两个码字的比特数之和　B．两个码字的比特数之差
C．两个码字之间相同的比特数　D．两个码字之间不同的比特数

（15）A．3　　B．4　　C．5　　D．6

**试题（14）、（15）分析**

海明距离是把一个有效码字变成另一个有效码字所要改变的位数。如果对于 $m$ 位的数据，增加 $k$ 位冗余位，则组成 $n=m+k$ 位的纠错码。对于 $2^m$ 个有效码字中的任意一个，都有 $n$ 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错误位。这样，对于一个有效码字总共有 $n+1$ 个可识别的码字。这 $n+1$ 个码字相对于其他 $2^m-1$ 个有效码字的距离都大于 1。这意味着总共有 $2^m(n+1)$个有效的或是可纠错的码字。显然这个数应小于等于码字的所有可能的个数，即 $2^n$。于是，我们有

$$2^m(n+1)<2^n$$

因为 $n=m+k$，得出

$$m+k+1<2^k$$

对于给定的数据位 $m$，上式给出了 $k$ 的下界，即要纠正单个错误，$k$ 必须取的最小值。本题中 $m=6$，所以 $k=4$。

**参考答案**

（14）D　（15）B

**试题（16）、（17）**

IPv4 的 D 类地址是组播地址，用作组标识符，其中 224.0.0.1 代表__（16）__，224.0.0.5 代表__（17）__。

（16）A．DHCP 服务器　　B．RIPv2 路由器
　　C．本地子网中的所有主机　　D．OSPF 路由器

（17）A．DHCP 服务器　　B．RIPv2 路由器
　　C．本地子网中的所有主机　　D．OSPF 路由器

**试题（16）、（17）分析**

IPv4 的 D 类地址是组播地址，用作一个组的标识符，其地址范围是 224.0.0.0～239.255.255.255。按照约定，D 类地址被划分为 3 类：

- 224.0.0.0～224.0.0.255：保留地址，用于路由协议或其他下层拓扑发现协议，以及维护管理协议等，例如 224.0.0.1 代表本地子网中的所有主机，224.0.0.2 代表本地子网中的所有路由器，224.0.0.5 代表所有 OSPF 路由器，224.0.0.5 代表所有 RIP 2 路由器，224.0.0.12 代表 DHCP 服务器或中继代理，224.0.0.13 代表所有支持 PIM 的路由器等。
- 224.0.1.0～238.255.255.255：用于全球范围的组播地址分配，可以把这个范围的 D 类地址动态地分配给一个组播组，当一个组播会话停止时，其地址被回收，以后还可以分配给新出现的组播组。
- 239.0.0.0～239.255.255.255：在管理权限范围内使用的组播地址，限制了组播的范围，可以在本地子网中作为组播地址使用。

**参考答案**

（16）C　（17）D

**试题（18）**

按照 IETF 定义的区分服务（DiffServ）技术规范，边界路由器要根据 IP 协议头中的__（18）__字段为每个 IP 分组打上一个称为 DS 码点的标记，这个标记代表了该分组的 QoS 需求。

（18）A．目标地址　　B．源地址　　C．服务类型　　D．段偏置值

**试题（18）分析**

区分服务（DiffServ）将具有相同特性的若干业务流汇聚起来，为整个汇聚流提供服务，而不是面向单个业务流来提供服务。

每个 IP 分组都要根据其 QoS 需求打上一个标记，这种标记称为 DS 码点（DS Code Point，DSCP），可以利用 IPv4 协议头中的服务类型（Type of Service）字段，或者 IPv6 协议头中的通信类别（Traffic Class）字段来实现，这样就维持了现有的 IP 分组格式不变。

在使用 DiffServ 服务之前，服务提供者与用户之间先要建立一个服务等级约定（Service Level Agreement，SLA）。这样，在各个应用中就不再需要类似的机制，从而可以保持现有的应用不变。

Internet 中能实现区分服务的连续区域被称为 DS 域（DS Domain），在一个 DS 域中，服务提供策略（Service Provisioning Policies）和逐跳行为（Per-Hop Behavior，PHB）都是一致的。PHB 是（外部观察到的）DS 结点对一个分组的转发行为。

**参考答案**

（18）C

**试题（19）、（20）**

ICMP 协议属于因特网中的__（19）__协议，ICMP 协议数据单元封装在__（20）__中传送。

（19）A．数据链路层　　B．网络层　　C．传输层　　D．会话层

（20）A．以太帧　　B．TCP 段　　C．UDP 数据报　　D. IP 数据报

**试题（19）、（29）分析**

ICMP（Internet control Message Protocol）与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠的提交。ICMP 报文有 11 种之多，报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

| 类　型 | 代　码 | 校验和 |
|---|---|---|
| 参　数 | | |
| 信息（可变长） | | |

图　ICMP 报文格式

**参考答案**

（19）B　（20）D

**试题（21）、（22）**

TCP/IP 网络中最早使用的动态路由协议是__（21）__协议，这种协议基于__（22）__算法来计算路由。

（21）A．RIP　　B．OSPF　　C．PPP　　D．IS-IS

（22）A．路由信息　　B．链路状态　　C．距离矢量　　D．最短通路

**试题（21）、（22）分析**

路由协议（routing protocol）是路由器之间实现路由信息共享的一种机制，它允许路由器之间通过交换路由信息动态地维护各自的路由表。IP 协议是根据路由表进行分组转发的协议，按照业内的说法，应该叫作被路由的协议（routed protocol）。

最早使用的路由协议是路由信息协议（Routing Information Protocol，RIP）。RIP 的原型出现在 UNIX Berkley 4.3 BSD 中，它采用 Bellman-Ford 的距离矢量路由算法，用于在 ARPAnet 中计算最佳路由，现在的 RIP 作为内部网关协议运行在基于 TCP/IP 的网络中。RIP 适用于小型网络，因为它允许的跳步数不超过 15 步。

**参考答案**

（21）A　（22）C

**试题（23）**

动态划分 VLAN 的方法中不包括__（23）__。

（23）A．网络层协议　　B．网络层地址　C．交换机端口　　D．MAC 地址

**试题（23）分析**

在交换机上实现 VLAN，可以采用静态的或动态的方法：

① 静态分配 VLAN：为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口所在的 VLAN。

② 动态分配 VLAN：动态 VLAN 通过网络管理软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址划分 VLAN 的方法应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的任何地方，接入交换机根据设备的 MAC 地址就可以确定该设备的 VLAN 成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的 VLAN。

但是当用户数量很多时，对每个用户设备分配 VLAN 的工作量是很大的管理负担。

**参考答案**

（23）C

**试题（24）、（25）**

在局域网中划分 VLAN，不同 VLAN 之间必须通过__（24）__连接才能互相通信。属于各个 VLAN 的数据帧必须打上不同的__（25）__。

（24）A. 中继端口　B. 动态端口　C. 接入端口　D. 静态端口

（25）A. VLAN 优先级　B. VLAN 标记

C. 用户标识　D. 用户密钥

**试题（24）、（25）分析**

在划分成 VLAN 的交换网络中，交换机端口之间的连接分为两种：接入链路（Access-Link Connection）和中继连接（Trunk Connection）。接入链路只能连接具有标准以太网卡的设备，也只能传送属于单个 VLAN 的数据包。任何连接到接入链路的设备都属于同一广播域，这意味着，如果有 10 个用户连接到一个集线器，而集线器被插入到交换机的接入链路端口，则这 10 个用户都属于该端口规定的 VLAN。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个 VLAN。在进入中继端口时，交换机在数据包中加入 VLAN 标记（IEEE 802.11q）。这样，在中继链路另一端的交换机就不仅根据目标地址，而且要根据数据包所属的 VLAN 进行转发决策。

为了与接入链路设备兼容，在数据包进入接入链路连接的设备时，交换机要删除 VLAN 标记，恢复原来的帧结构。添加和删除 VLAN 标记的过程是由交换机中的专用硬件自动实现的，处理速度很快，不会引入太大的延迟。从用户角度看，数据源产生标准的以太帧，目标接收的也是标准的以太帧，VLAN 标记对用户是透明的。

**参考答案**

（24）A　（25）B

**试题（26）、（27）**

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE802.1ad 定义的运营商网桥协议提供的基本技术是在以太帧中插入__（26）__字段，这种技术被称为__（27）__技术。

（26）A. 运营商 VLAN 标记　B. 运营商虚电路标识

C. 用户 VLAN 标记　D. 用户帧类型标记

（27）A. Q-in-Q　B. IP-in-IP

C. NAT-in-NAT　D. MAC-in-MAC

**试题（26）、（27）分析**

城域以太网论坛（Metro Ethernet Forum，MEF）提出以太局域网服务（E-LAN services）是指，由运营商建立一个城域以太网，在用户以太网之间提供多点对多点的第

二层连接，任意两个以太网用户之间都可以通过城域以太网通信。

提供 E-LAN 服务的基本技术是 802.1q 的 VLAN 帧标记。我们假定，各个用户的以太网称为 C-网，运营商建立的城域以太网称为 S-网。如果不同 C-网中的用户要进行通信，以太帧在进入用户网络接口（User-Network Interface，UNI）时被插入一个 S-VID（Server Provider-VLAN ID）字段，用于标识 S-网中的传输服务，而用户的 VLAN 帧标记（C-VID）则保持不变，当以太帧到达目标 C-网时，S-VID 字段被删除，如下图所示。这样就解决了两个用户以太网之间透明的数据传输问题。这种技术定义在 IEEE802.1ad 的运营商网桥协议（Provider Bridge Protocol）中，被称为 Q-in-Q 技术。

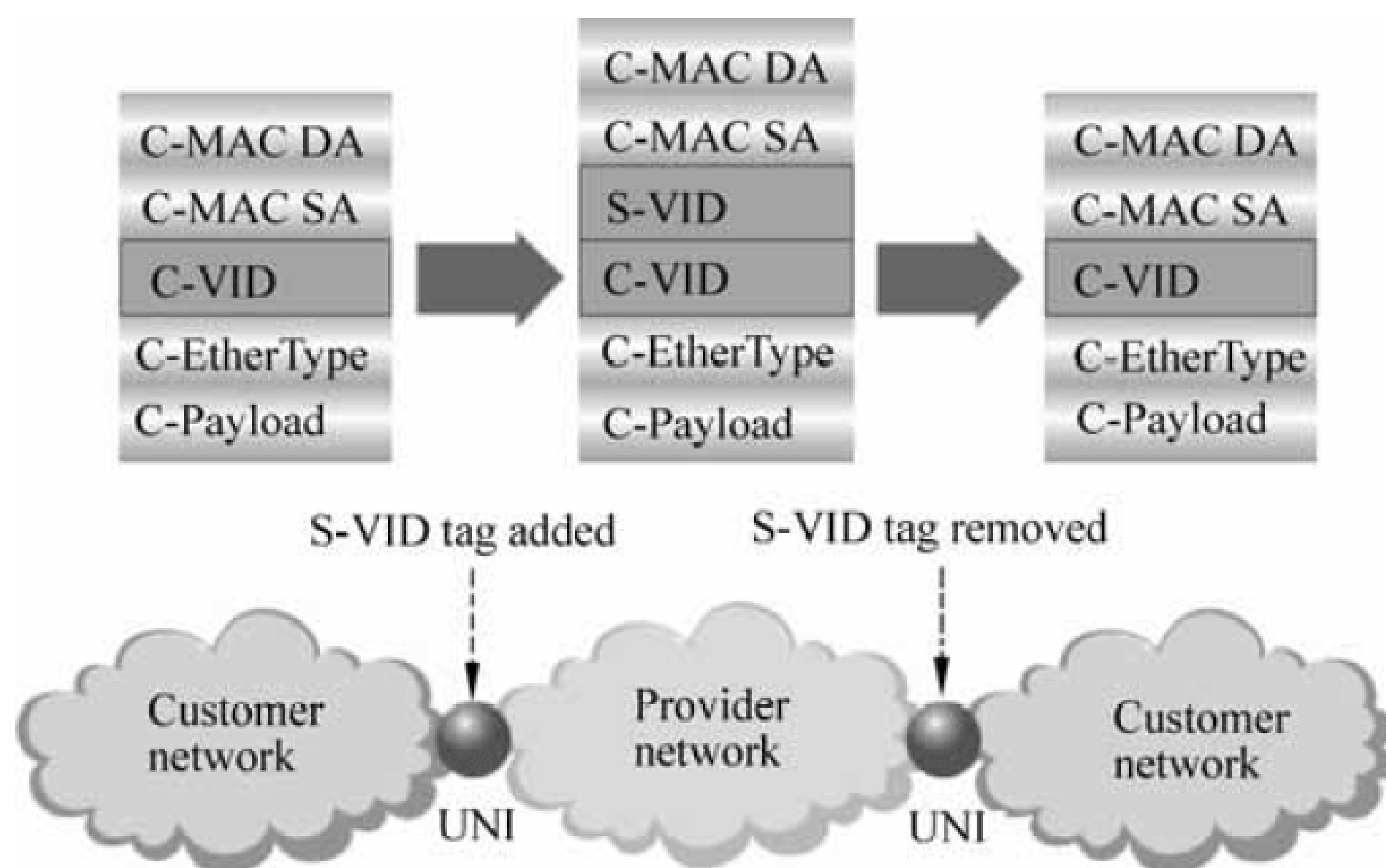



图　802.1ad 的帧格式

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，由于其简单性和有效性而得到电信运营商的青睐。但是这样一来，所有用户的 MAC 地址在城域以太网中都是可见的，任何 C-网的改变都会影响到 S-网的配置，增加了管理的难度。而且 S-VID 字段只有 12 位，只能标识 4096 个不同的传输服务，网络的可扩展性也受到限制。从用户角度看，网络用户的 MAC 地址都暴露在整个城域以太网中，使得网络的安全性受到威胁。

为了解决上述问题，IEEE 802.1ah 标准提出了运营商主干网桥（Provider Backbone Bridge，PBB）协议。所谓主干网桥就是运营商网络边界的网桥，通过 PBB 对用户以太帧再封装一层运营商的 MAC 帧头，添加主干网目标地址和源地址（B-DA，B-SA）、主干网 VLAN 标识（B-VID），以及服务标识（I-SID）等字段。由于用户以太帧被封装在主干网以太帧中，所以这种技术被称为 MAC-in-MAC 技术。

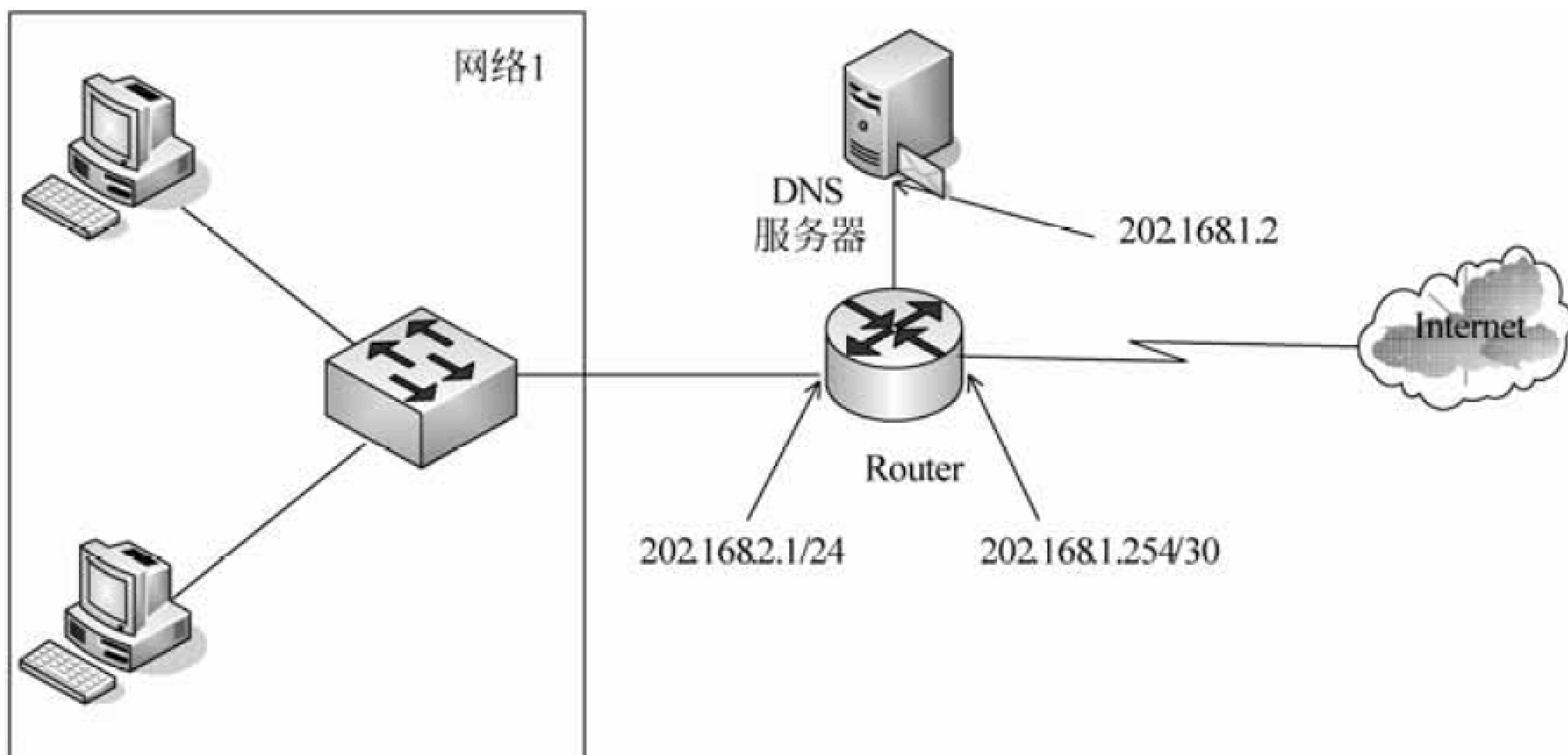
**参考答案**

（26）A　（27）A

**试题（28）、（29）**

网络配置如下图所示，在路由器 Router 中配置网络 1 访问 DNS 服务器的主机路由

的命令是___（28）___。网络 1 访问 Internet 的默认路由命令是___（29）___。




（28）A. ip　route　202.168.1.2　255.255.255.0　202.168.1.2
　　B. ip　route　202.168.1.2　255.255.255.255　202.168.1.2
　　C. ip　route　0.0.0.0　0.0.0.0　202.168.1.253
　　D. ip　route　255.255.255.255　0.0.0.0　202.168.1.254

（29）A. ip　route　202.168.1.2　255.255.255.0　202.168.1.2
　　B. ip　route　202.168.1.2　255.255.255.255　202.168.1.2
　　C. ip　route　0.0.0.0　0.0.0.0　202.168.1.253
　　D. ip　route　255.255.255.255　0.0.0.0　202.168.1.254

**试题（28）、（29）分析**

本试题考查静态路由配置命令。

网络 1 访问 DNS 服务器时目的网络是 DNS 服务器单个 IP，地址为 202.168.1.2，路由器转发的是下一跳即为 202.168.1.2，故命令为 ip route 202.168.1.2 255.255.255.255 202.168.1.2。

网络 1 访问 Internet 时，地址任意，路由时下一跳为 202.168.1.253，故默认路由为 ip　route　0.0.0.0　0.0.0.0　202.168.1.253。

**参考答案**

（28）B　（29）C

**试题（30）**

与 HTTP1.0 相比，HTTP 1.1 的优点不包括___（30）___。

（30）A. 减少了 RTTs 数量　　B. 支持持久连接
　　C. 减少了 TCP 慢启动次数　　D. 提高了安全性

**试题（30）分析**

与 HTTP1.0 相比，HTTP 1.1 最大的改进是支持持久连接，从而减少了 TCP 慢启动

的次数，进而减少了 RTTs 数量。

**参考答案**

（30）D

**试题（31）**

在运行 Linux 系统的服务器中，使用 BIND 配置域名服务，主配置文件存放在<u>（31）</u>中。

（31）A．name.conf　　B．named.conf　　C．dns.conf　　D．dnsd.conf

**试题（31）分析**

BIND 是 Linux 系统中常用的域名配置组件，主配置为 named.conf。

**参考答案**

（31）B

**试题（32）**

在 Linux 系统中，root 用户执行 shutdown -r now 命令，系统将会<u>（32）</u>。

（32）A．重新启动　　B．进入单用户模式　　C．休眠　　D．关机

**试题（32）分析**

Linux 系统中采用 shutdown -r now 命令重新启动系统。

**参考答案**

（32）A

**试题（33）**

结构化综合布线系统中的干线子系统是指<u>（33）</u>。

（33）A．管理楼层内各种设备的子系统

B．连接各个建筑物的子系统

C．工作区信息插座之间的线缆子系统

D．实现楼层设备间连接的子系统

**试题（33）分析**

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如下图所示。

① 工作区子系统（Work Location）。

工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器以及传感器等多种终端设备。

② 水平布线子系统（Horizontal）。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平子系统的作用是将干线子系统线路延伸到用户工作区。在进行水平布线时，传输介质中间不宜有转折点，两端应直接从配线架连接到工作区的信息插座。水平布线的布线通

道有两种：一种是暗管预埋、墙面引线方式，另一种是地下管槽、地面引线方式。前者适用于多数建筑系统，一旦铺设完成，不易更改和维护；后者适合于少墙多柱的环境，更改和维护方便。

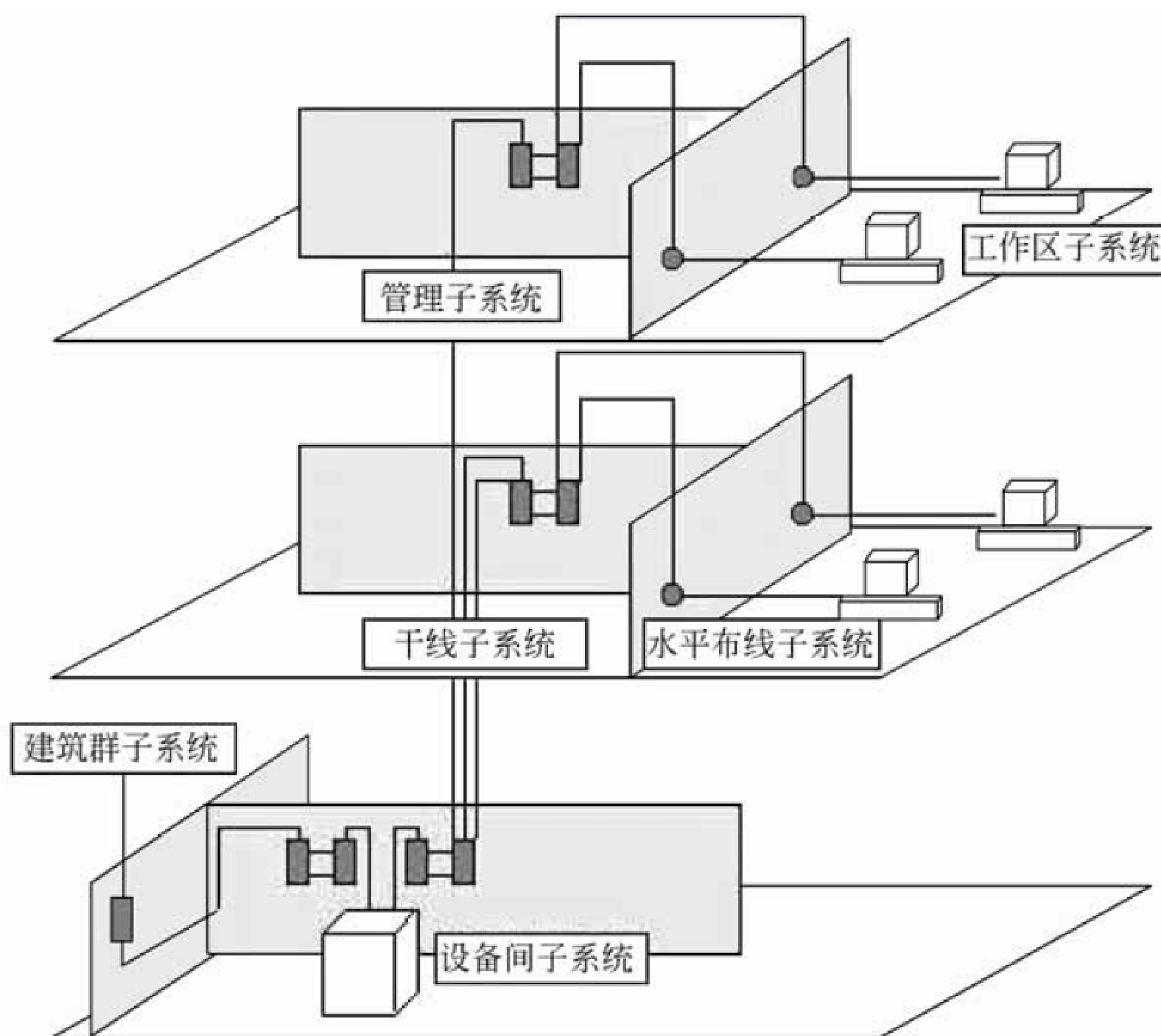



图　结构化布线示意图

③ 管理子系统（Administration）。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆互连，这些短线被称为跳线。通过跳线的调整，可以对工作区的信息插座和交换机端口之间进行连接切换。

④ 干线子系统（Backbone）。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。主干子系统在设计时，对于旧建筑物，主要采用楼层牵引管方式铺设，对于新建筑物，则利用建筑物的线井进行铺设。

⑤ 设备间子系统（Equipment）。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交

换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX、网络设备和监控设备等）之间的连接。

⑥ 建筑群子系统（Campus）。

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。大楼之间的布线方法有三种，一种是地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各种规定，安装时至少应预留 1 到 2 个备用管孔，以备扩充之用。第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志。最后一种是架空明线，这种方法需要经常维护。

**参考答案**

（33）D

**试题（34）**

假设网络的生产管理系统采用 B/S 工作方式，经常上网的用户数为 100 个，每个用户每分钟平均产生 11 个事务，平均事务量大小为 0.06Mb，则这个系统需要的信息传输速率为__（34）__。

（34）A. 5.28Mb/s　　B. 8.8Mb/s　　C. 66Mb/s　　D. 528Mb/s

**试题（34）分析**

系统需要的信息传输速率 R=0.06MB×8×11×100÷60= 8.8Mb/s

**参考答案**

（34）B

**试题（35）**

在 Windows 命令行窗口中进入 nslookup 交互工作方式，然后输入 set type=mx，这样的设置可以__（35）__。

（35）A. 切换到指定的域名服务器　　B. 查询邮件服务器的地址

C. 由地址查找对应的域名　　D. 查询域名对应的各种资源

**试题（35）分析**

Nslookup 命令用于显示 DNS 查询信息，诊断和排除 DNS 故障，有交互式和非交互式两种工作方式。

所谓非交互式工作就是只使用一次 Nslookup 命令后又返回到 Cmd.exe 提示符下。Nslookup 命令后面可以跟随一个或多个命令行选项，用于设置查询参数。每个命令行的各选项由一个连字符“-”后跟选项的名字，有时还要加一个等号“=”和一个数值。例如应用默认的 DNS 服务器由域名查找 IP 地址。

```
C:\>nslookup ns1.isi.edu
Server: ns1.domain.com
Address: 202.30.19.1
```

```
Non-authoritative answer:    #给出应答的服务器不是该域的权威服务器
Name: ns1.isi.edu
Address: 128.9.0.107         #查出的 IP 地址
```

如果需要查找多项数据，可以使用 Nslookup 的交互工作方式。在 Cmd.exe 提示符下输入 nslookup 后回车，就进入了交互工作方式，命令提示符变成“>”。在命令提示符“>”下输入 help 或?，会显示可用的命令列表，如果输入 exit，则返回 Cmd.exe 提示符。

在交互方式下，可以用 set 命令设置选项，满足指定的查询需要。例如查询本地域的邮件交换器信息的过程如下。

```
C:\> nslookup
Default Server: ns1.domain.com
Address: 202.30.19.1
> set type=mx
> 163.com.cn
Server: ns1.domain.com
Address: 202.30.19.1

Non-authoritative answer:
163.com.cn      MX preference = 10, mail exchanger =mx1.163.com.cn
163.com.cn      MX preference = 20, mail exchanger =mx2.163.com.cn
mx1.163.com.cn  internet address = 61.145.126.68
mx2.163.com.cn  internet address = 61.145.126.30
>
```

**参考答案**

（35）B

**试题（36）**

FTP 提供了丰富的命令，用来更改本地计算机工作目录的命令是__（36）__。

（36）A．get　　B．list　　C．lcd　　D．!list

**试题（36）分析**

FTP 用来更改本地计算机工作目录的命令是 lcd。

**参考答案**

（36）C

**试题（37）**

在进行域名解析的过程中，由__（37）__获取的解析结果耗时最短。

（37）A．主域名服务器　　B．辅域名服务器

C．本地缓存　　D．转发域名服务器

**试题（37）分析**

域名解析的过程是先查本地缓存，再查主域名服务器；若主域名服务器查找不到记录，转到转发域名服务器进行查询；若主域名服务器不工作，启用辅域名服务器进行查询。不论是主域名服务器、转发域名服务器还是辅域名服务器，都需要在资源记录数据库中去匹配，时间较本地缓存要长。

**参考答案**

（37）C

**试题（38）**

DNS 通知是一种推进机制，其作用是使得__（38）__。

（38）A．辅助域名服务器及时更新信息
B．授权域名服务器向管区内发送公告
C．本地域名服务器发送域名解析申请
D．递归查询迅速返回结果

**试题（38）分析**

DNS 通知机制的作用是使得辅助域名服务器及时更新信息。

**参考答案**

（38）A

**试题（39）**

在 DNS 资源记录中，__（39）__记录类型的功能是把 IP 地址解析为主机名。

（39）A．A　　B．NS　　C．CNAME　　D．PTR

**试题（39）分析**

在 DNS 资源记录中，记录类型 A 的功能是域名映射为 IP 地址；记录类型 NS 的功能是给出区域的授权服务器；记录类型 CNAME 的功能是为正式主机名（canonical name）定义了一个别名（alias）；记录类型 PTR 的功能是把 IP 地址解析为主机名。

**参考答案**

（39）D

**试题（40）**

以下关于 DHCP 的描述中，正确的是__（40）__。

（40）A．DHCP 客户机不可跨网段获取 IP 地址
B．DHCP 客户机只能收到一个 dhcpoffer
C．DHCP 服务器可以把一个 IP 地址同时租借给两个网络的不同主机
D．DHCP 服务器中可自行设定租约期

**试题（40）分析**

DHCP 客户机可通过配置 DHCP 中继跨网段获取 IP 地址；DHCP 客户机可能收到一个 dhcpoffer，通常选择最先到达的 dhcpoffer 提供的地址；DHCP 服务器把一个 IP 地址

只能租借给一台主机；DHCP 服务器中可自行设定租约期。

**参考答案**

（40）D

**试题（41）**

高级加密标准 AES 支持的 3 种密钥长度中不包括__（41）__位。

（41）A．56　　B．128　　C．192　　D．256

**试题（41）分析**

本题考查数据加密算法的基础知识。

1997 年 1 月，美国国家标准与技术局（NIST）为高级加密标准征集新算法。最初从许多响应者中挑选了 15 个候选算法，经过了世界密码共同体的分析，选出了其中的 5 个。经过用 ANSI C 和 Java 语言对 5 个算法的加/解密速度、密钥和算法的安装时间，以及对各种攻击的拦截程度等进行了广泛的测试后，2000 年 10 月，NIST 宣布 Rijndael 算法为 AES 的最佳候选算法，并于 2002 年 5 月 26 日发布正式的 AES 加密标准。

AES 支持 128，192 和 256 位三种密钥长度，能够在世界范围内免版税使用，提供的安全级别足以保护未来 20～30 年内的数据，可以通过软件或硬件实现。

**参考答案**

（41）A

**试题（42）**

在报文摘要算法 MD5 中，首先要进行明文的分组与填充，其中分组时明文报文要按照__（42）__位分组。

（42）A．128　　B．256　　C．512　　D．1024

**试题（42）分析**

本题考查报文摘要算法的基础知识。

报文摘要算法 MD5 的基本思想就是用足够复杂的方法把报文位充分“弄乱”，使得每一个输出位都受到每一个输入位的影响。具体的操作分成下列步骤：

① 分组和填充：把明文报文按 512 位分组，最后要填充一定长度的“1000....”，使得报文长度=448（mod 512）

② 附加。最后加上 64 位的报文长度字段，整个明文恰好为 512 的整数倍。

③ 初始化。置 4 个 32 位长的缓冲区 ABCD 分别为：

A=01234567　B=89ABCDEF　C=FEDCBA98　D=76543210

④ 处理。用 4 个不同的基本逻辑函数（F，G，H，I）进行 4 轮处理，每一轮以 ABCD 和当前 512 位的块为输入，处理后送入 ABCD（128 位），产生 128 位的报文摘要。

**参考答案**

（42）C

**试题（43）**

以下关于 IPSec 协议的描述中，正确的是__（43）__。

（43）A．IPSec 认证头（AH）不提供数据加密服务

B．IPSec 封装安全负荷（ESP）用于数据完整性认证和数据源认证

C．IPSec 的传输模式对原来的 IP 数据报进行了封装和加密，再加上了新的 IP 头

D．IPSec 通过应用层的 Web 服务建立安全连接

**试题（43）分析**

本题考查 IPsec 协议的基础知识。

IPSec 的功能可以划分为三类：① 认证头（Authentication Header，AH）：用于数据完整性认证和数据源认证。② 封装安全负荷（Encapsulating Security Payload，ESP）：提供数据保密性和数据完整性认证，ESP 也包括了防止重放攻击的顺序号。③ Internet 密钥交换协议（Internet Key Exchange，IKE）：用于生成和分发在 ESP 和 AH 中使用的密钥，IKE 也对远程系统进行初始认证。

IPSec 在传输模式，IP 头没有加密，只对 IP 数据进行了加密；在隧道模式，IPSec 对原来的 IP 数据报进行了封装和加密，加上了新的 IP 头。

IPSec 的安全头插入在标准的 IP 头和上层协议（例如 TCP）之间，任何网络服务和网络应用可以不经修改地从标准 IP 转向 IPSec，同时 IPSec 通信也可以透明地通过现有的 IP 路由器。

**参考答案**

（43）A

**试题（44）**

防火墙的工作层次是决定防火墙效率及安全的主要因素，下面的叙述中正确的是__（44）__。

（44）A．防火墙工作层次越低，工作效率越高，安全性越高

B．防火墙工作层次越低，工作效率越低，安全性越低

C．防火墙工作层次越高，工作效率越高，安全性越低

D．防火墙工作层次越高，工作效率越低，安全性越高

**试题（44）分析**

本题考查防火墙的基础知识。

防火墙的性能及特点主要由以下两方面所决定。

① 工作层次。这是决定防火墙效率及安全的主要因素。一般来说，工作层次越低，则工作效率越高，但安全性就低了；反之，工作层次越高，工作效率越低，则安全性越高。

② 防火墙采用的机制。如果采用代理机制，则防火墙具有内部信息隐藏的特点，相对而言，安全性高，效率低；如果采用过滤机制，则效率高，安全性却降低了。

**参考答案**

（44）D

**试题（45）**

在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法中不包括__（45）__。

（45）A．模式匹配　B．密文分析　C．数据完整性分析　D．统计分析

**试题（45）分析**

本题考查入侵检测系统的基础知识。

入侵检测系统由 4 个模块组成：事件产生器、事件分析器、事件数据库和响应单元。其中，事件分析器负责接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其分析方法有三种：

① 模式匹配：将收集到的信息与已知的网络入侵数据库进行比较，从而发现违背安全策略的行为。

② 统计分析：首先给系统对象（例如用户、文件、目录和设备等）建立正常使用时的特征文件（Profile），这些特征值将被用来与网络中发生的行为进行比较。当观察值超出正常值范围时，就认为有可能发生入侵行为。

③ 数据完整性分析：主要关注文件或系统对象的属性是否被修改，这种方法往往用于事后的审计分析。

**参考答案**

（45）B

**试题（46）**

在 Windows Server 2003 环境中有本地用户和域用户两种用户。其中本地用户信息存储在__（46）__。

（46）A．本地计算机的 SAM 数据库　B．本地计算机的活动目录
C．域控制器的活动目录　D．域控制器的 SAM 数据库

**试题（46）分析**

本题考查 Windows Server 2003 的相关网络管理知识。

在 Windows Server 2003 环境中有本地用户和域用户两种用户。本地用户信息存储在本地计算机的安全账户管理器（Security Accounts Manager，SAM）数据库内，当本地计算机用户尝试本地登录时，SAM 数据库中的账户信息要经过验证。域用户信息存储在域控制器的活动目录中。活动目录是网络中的一个中央数据库，存储各种资源信息。

**参考答案**

（46）A

**试题（47）**

管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他

行的索引值不冲突，则代理产生一个新行，其状态对象的值为__（47）__。

（47）A. createRequest　　B. underCreate
　　　C. valid　　D. invalid

**试题（47）分析**

本题考查 RMON 的基本知识。

管理站用 Set 命令在 RMON 表中增加新行，遵循的规则是：管理站用 SetRequest 在 RMON 表中产生一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理产生一个新行，其状态对象的值为 createRequest。

**参考答案**

（47）A

**试题（48）**

SNMPc 支持各种设备访问方式，在 SNMPc 支持的设备访问方式中，只是用于对 TCP 服务轮询的方式是__（48）__。

（48）A. 无访问模式　　B. ICMP（Ping）
　　　C. SNMPv1 和 v2C　　D. SNMPv3

**试题（48）分析**

本题考查网络管理软件 SNMPc 的设备访问模式。

SNMPc 支持各种设备访问方式，包括 TCP、ICMP（Ping）、SNMPv1、SNMPv2C 和 SNMPv3。其中无访问模式（仅对 TCP）：无访问模式只是用于对 TCP 服务的轮询，当 ICMP/SNMP 访问受防火墙限制时使用这种方式。 ICMP（Ping）：ICMP（Ping）用于不支持 SNMP 但仍可通过 Ping 测试其是否有响应的设备。此类设备也可能包括服务器和工作站。SNMPv1 和 v2C：SNMPv1 和 SNMP v2C 是非常相似的 SNMP 代理协议，目前部署的网络设备大多数都使用这两种协议。任何支持 v2C 的设备一般同样也支持 v1。SNMPc 根据需要在两种方式之间自动智能切换。因此在多数情况下总是会选择 SNMPv1 作为设备的访问方式。 SNMP v3：SNMP v3 是安全的 SNMP 代理协议，支持身份验证和加密功能。

**参考答案**

（48）A

**试题（49）**

下列数据类型中，SNMPv2 支持而 SNMPv1 不支持的是__（49）__。

（49）A. OCTET STRING　　B. OBJECT descriptor
　　　C. Unsigned32　　D. Gauge32

**试题（49）分析**

本题考查 SNMPv1 和 SNMPv2 的数据类型。SNMPv2 增加了两种新的数据类型 Unsigned32 和 Counter64。这两种是 SNMPv2 支持而 SNMPv1 不支持的数据类型。

**参考答案**

（49）C

**试题（50）**

某实验室使用无线路由器提供内部上网，无线路由器采用固定 IP 地址连接至校园网，实验室用户使用一段时间后，不定期出现不能访问互联网的现象，经测试无线路由器工作正常，同时有线接入的用户可以访问互联网。分析以上情况，导致这一故障产生的最可能的原因是＿（50）＿。

（50）A．无线路由器配置错误　　B．无线路由器硬件故障

C．内部或者外部网络攻击　　D．校园网接入故障

**试题（50）分析**

本题考查网络故障分析的相关知识。

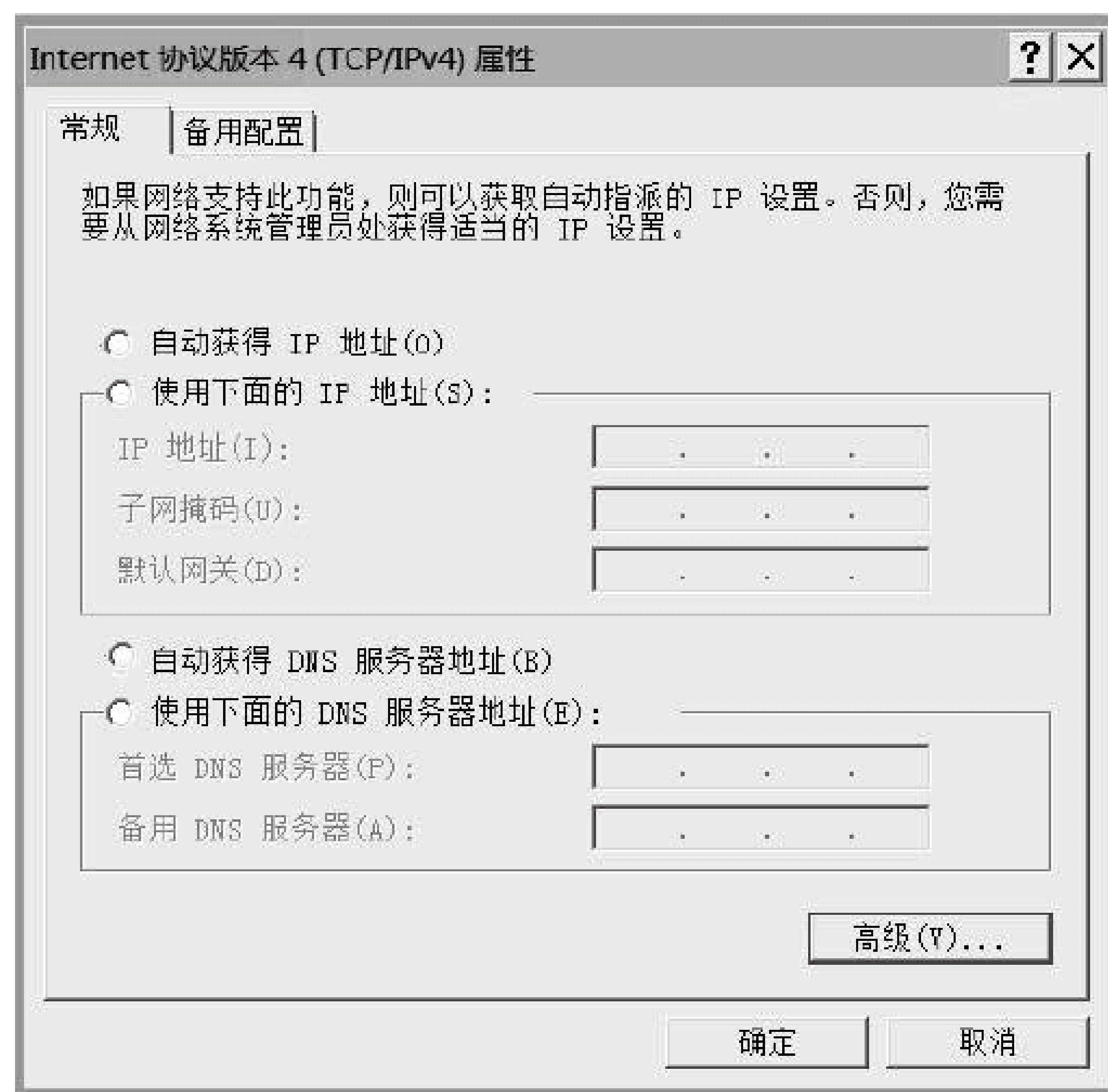
根据题目经测试无线路由器工作正常则说明无线路由器硬件无故障，而如果是配置错误则不会出现实验室用户使用一段时间后，不定期出现不能访问互联网的现象。另外题目说同时有线接入的用户可以访问互联网，说明校园网接入服务正常。而如果有在该路由器受到实验室内部或者外部的网络攻击时则很有可能产生此现象。

**参考答案**

（50）C

**试题（51）**

校园网连接运营商的 IP 地址为 202.117.113.3/30，本地网关的地址为 192.168.1.254/24，如果本地计算机采用动态地址分配，在下图中应如何配置？＿（51）＿。




（51）A．选取“自动获得 IP 地址”

B．配置本地计算机 IP 地址为 192.168.1.×

C. 配置本地计算机 IP 地址为 202.115.113.×

D. 在网络 169.254.×.×中选取一个不冲突的 IP 地址

**试题（51）分析**

如果采用动态地址分配方案，本地计算机应设置为“自动获得 IP 地址”。

**参考答案**

（51）A

**试题（52）**

下面的选项中，不属于网络 202.113.100.0/21 的地址是__（52）__。

（52）A. 202.113.102.0　　B. 202.113.99.0

C. 202.113.97.0　　D. 202.113.95.0

**试题（52）分析**

网络地址 202.113.100.0/21 的二进制为：　**11001010 01110001 01100**100 00000000

地址 202.113.102.0 的二进制为：　11001010 01110001 01100110 00000000

地址 202.113.99.0 的二进制为：　11001010 01110001 01100011 00000000

地址 202.113.97.0 的二进制为：　11001010 01110001 01100001 00000000

地址 202.113.95.0 的二进制为：　11001010 01110001 01011111 00000000

可以看出，地址 202.113.95.0 不属于网络 202.113.100.0/21。

**参考答案**

（52）D

**试题（53）、（54）**

IP 地址块 112.56.80.192/26 包含了__（53）__个主机地址，不属于这个网络的地址是__（54）__。

（53）A. 15　　B. 32　　C. 62　　D. 64

（54）A. 112.56.80.202　　B. 112.56.80.191

C. 112.56.80.253　　D. 112.56.80.195

**试题（53）、（54）分析**

地址块 112.56.80.192/26 包含了 6 位主机地址，所以包含的主机地址为 62 个。

网络地址 112.56.80.192/26 的二进制为：　**01110000 00111000 01010000 11**000000

地址 112.56.80.202 的二进制为：　01110000 00111000 01010000 11001010

地址 112.56.80.191 的二进制为：　01110000 00111000 01010000 10111111

地址 112.56.80.253 的二进制为：　01110000 00111000 01010000 11111101

地址 112.56.80.195 的二进制为：　01110000 00111000 01010000 11000011

可以看出，地址 112.56.80.191 不属于网络 112.56.80.192/26。

**参考答案**

（53）C　（54）B

**试题（55）**

下面的地址中属于单播地址的是__（55）__。

（55）A．125.221.191.255/18　　B．192.168.24.123/30
　　C．200.114.207.94/27　　D．224.0.0.23/16

**试题（55）分析**

地址 125.221.191.255/18 的二进制为：　**01111101 11001101 10**111111 11111111

地址 192.168.24.123/30 的二进制为：　**11000000 10101000 00011000 011110**11

地址 200.114.207.94/27 的二进制为：　**11001000 00111000 01110010 110**11110

地址 224.0.0.23/16 二进制为：　**11100000 00000000** 00000000 00010111

可以看出 125.221.191.255/18 和 192.168.24.123/30 都是广播地址，而 224.0.0.23/16 是组播地址，只有 200.114.207.94/27 是单播地址。

**参考答案**

（55）C

**试题（56）**

IPv6 地址的格式前缀用于表示地址类型或子网地址，例如 60 位的地址前缀 12AB00000000CD3 有多种合法的表示形式，下面的选项中，不合法的是__（56）__。

（56）A．12AB:0000:0000:CD30:0000:0000:0000:0000/60
　　B．12AB::CD30:0:0:0:0/60
　　C．12AB:0:0:CD3/60
　　D．12AB:0:0:CD30::/60

**试题（56）分析**

IPv6 地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可表示为“IPv6 地址/前缀长度”的形式。例如 60 位的地址前缀 12AB00000000CD3 有下列几种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

下面的表示形式是不合法的：

12AB:0:0:CD3/60　（在 16 比特的字段中可以省掉前面的 0，但不能省掉后面的 0）

12AB::CD30/60（这种表示可展开为 12AB:0000:0000:0000:0000:0000:0000:CD30）

12AB::CD3/60（这种表示可展开为 12AB:0000:0000:0000:0000:0000:0000:0CD3）

**参考答案**

（56）C

**试题（57）**

IPv6 新增加了一种任意播地址，这种地址__（57）__。

（57）A. 可以用作源地址，也可以用作目标地址
B. 只可以作为源地址，不能作为目标地址
C. 代表一组接口的标识符
D. 可以用作路由器或主机的地址

**试题（57）分析**

任意播（AnyCast）地址是一组接口（可属于不同结点的）的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对 IPv6 任意播地址存在下列限制：

- 任意播地址不能用作源地址，而只能作为目标地址；
- 任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

**参考答案**

（57）C

**试题（58）、（59）**

所谓移动 IP 是指＿（58）＿；实现移动 IP 的关键技术是＿（59）＿。

（58）A. 通过地址翻译技术改变主机的 IP 地址
B. 一个主机的 IP 地址可以转移给另一个主机
C. 移动主机通过在无线通信网中漫游来保持网络连接
D. 移动主机在离开家乡网络的远程站点可以连网工作

（59）A. 移动主机具有一个可以接入任何网络的通用 IP 地址
B. 移动主机具有一个家乡网络地址并获取一个外地转交地址
C. 移动主机通过控制全网的管理中心申请网络接入服务
D. 移动主机总是通过家乡网络地址来获取接入服务

**试题（58）、（59）分析**

通常在联网的计算机中，有一类主机用铜缆或光纤连接在局域网中，从来不会移动，我们认为这些主机是静止的。可以移动的主机有两类，一类基本上是静止的，只是有时候从一个地点移动到另一个地点，并且在任何地点都可以通过有线或无线连接进入 Internet；另一类是在运动中进行计算的主机，它通过在无线通信网中漫游来保持网络连接。为解决前一类偶尔移动的主机异地联网的问题，IETF 成立了专门的工作组，并预设了下列研究目标：

- 移动主机能够在任何地方使用它的家乡地址进行连网；
- 不允许改变主机中的软件；
- 不允许改变路由器软件和路由表的结构；
- 发送给移动主机的大部分分组不需要重新路由；
- 移动主机在家乡网络中的上网活动无须增加任何开销。

IETF 给出的解决方案是 RFC 3344（IP Mobility Support for IPv4）和 RFC 3775

(Mobility Support in IPv6)。RFC 3344 增强了 IPv4 协议，使其能够把 IP 数据报路由到移动主机当前所在的连接站点。按照这个方案，每个移动主机配置了一个家乡地址（home address）作为永久标识。当移动主机离开家乡网络时，通过所在地点的外地代理，它被赋予了一个转交地址（care-of address）。协议提供了一种注册机制，使得移动主机可以通过家乡地址获得转交地址。家乡代理通过安全隧道可以把分组转发给外地代理，然后被提交给移动主机。

**参考答案**

（58）D　（59）B

**试题（60）**

中国自主研发的 3G 通信标准是＿（60）＿。

（60）A．CDMA2000　　B．TD-SCDMA
　　　C．WCDMA　　D．WiMAX

**试题（60）分析**

1985 年，ITU 提出了对第三代移动通信标准的需求，1996 年正式命名为 IMT-2000（International Mobile Telecommunications-2000），其中的 2000 有 3 层含义：

- 使用的频段在 2000MHz 附近
- 通信速率于约为 2000kb/s（即 2Mb/s）
- 预期在 2000 年推广商用，1999 年 ITU 批准了五个 IMT-2000 的无线电接口，这五个标准是：
  - IMT-DS（Direct Spread）：即W-CDMA，属于频分双工模式，在日本和欧洲制定的UMTS系统中使用。
  - IMT-MC（Multi-Carrier）：即CDMA-2000，属于频分双工模式，是第二代CDMA系统的继承者。
  - IMT-TC（Time-Code）：这一标准是中国提出的TD-SCDMA，属于时分双工模式。
  - IMT-SC（Single Carrier）：也称为EDGE，是一种2.75G技术。
  - IMT-FT（Frequency Time）：也称为DECT。

2007 年 10 月 19 日，ITU 会议批准移动WiMAX作为第 6 个 3G 标准，称为 IMT-2000 OFDMA TDD WMAN，即无线城域网技术。

第三代数字蜂窝通信系统提供第二代蜂窝通信系统提供的所有业务类型，并支持移动多媒体业务。在高速车辆行驶时支持 144kb/s 的数据速率，步行和慢速移动环境下支持 384kb/s 的数据速率，室内静止环境下支持 2Mb/s 的高速数据传输，并保证可靠的服务质量。

**参考答案**

（60）B

**试题（61）**

IEEE 802.11 规定了多种 WLAN 通信标准，其中 （61） 与其他标准采用的频段不同，因而不能兼容。

（61）A. IEEE 802.11a　　B. IEEE 802.11b
　　C. IEEE 802.11g　　D. IEEE 802.11n

**试题（61）分析**

1990 年，IEEE 802.11 小组正式从事制定 WLAN 的物理层和 MAC 层标准的工作。1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM（Industrial Scientific and Medical）频段，采用扩频通信技术，支持 1Mb/s 和 2Mb/s 数据速率。1998 年推出的 IEEE 802.11b 标准也是运行在 ISM 频段，采用 CCK（Complementary Code Keying）调制技术，支持 11Mb/s 的数据速率。1999 年推出的 IEEE 802.11a 标准运行在 U-NII（Unlicensed National Information Infrastructure）频段，采用 OFDM 调制技术，支持最高达 54Mb/s 的数据速率，但是与 IEEE 802.11b/g 不兼容。2003 年推出的 IEEE802.11g 标准运行在 ISM 频段，与 IEEE 802.11b 兼容，数据速率提高到 54Mb/s。早期的 WLAN 标准主要有 4 种，如下表所示。

**IEEE 802.11 标准**

| 名　称 | 发布时间 | 工 作 频 段 | 调制技术 | 数 据 速 率 |
|---|---|---|---|---|
| 802.11 | 1997 年 | 2.4GHz ISM 频段 | DB/SK<br>DQPSK | 1Mb/s<br>2Mb/s |
| 802.11b | 1998 年 | 2.4GHz ISM 频段 | CCK | 5.5Mb/s，11Mb/s |
| 802.11a | 1999 年 | 5GHz U-NII 频段 | OFDM | 54Mb/s |
| 802.11g | 2003 年 | 2.4GHz ISM 频段 | OFDM | 54Mb/s |

2009 年 9 月 11 日 IEEE 802.11n 标准的正式发布。802.11n 可以将 WLAN 的传输速率由目前 802.11a/802.11g 的 54Mb/s 提高到 300Mb/s，甚至 600Mb/s。这个成就主要得益于 MIMO 与 OFDM 技术的结合。应用先进的无线通信技术，不但提高了传输速率，也极大地提升了传输质量。

**参考答案**

（61）A

**试题（62）、（63）**

IEEE 802.11 定义的 Ad Hoc 网络是由无线移动结点组成的对等网，这种网络的特点是 （62） 。在这种网络中使用的 DSDV（Destination-Sequenced Distance Vector）路由协议是一种 （63） 。

（62）A. 每个结点既是主机，又是交换机
　　B. 每个结点既是主机，又是路由器

C．每个结点都必须通过中心结点才能互相通信

D．每个结点都发送 IP 广播包来与其他结点通信

（63）A．洪泛式路由协议　　B．随机式路由协议

C．链路状态路由协议　　D．距离矢量路由协议

**试题（62）、（63）分析**

IEEE 802.11 标准定义的 Ad Hoc 网络是由无线移动结点组成的对等网，无须网络基础设施的支持，能够根据通信环境的变化实现动态重构，提供基于多跳无线连接的分组数据传输服务。在这种网络中，每一个结点既是主机，又是路由器，它们之间相互转发分组，形成一种自组织的 MANET（Mobile Ad Hoc Network）网络。

路由算法是 MANET 网络中重要的组成部分，传统有线网络的路由协议不能直接应用于 MANET。目标排序的距离矢量协议（Destination-Sequenced Distance Vector，DSDV）是一种扁平式路由协议。这是由传统的 Bellman-Ford 算法改进的距离矢量协议，利用序列号机制解决了路由环路问题，对后来的协议设计有很大影响。

**参考答案**

（62）B　（63）D

**试题（64）、（65）**

OSPF 协议将其管理的网络划分为不同类型的若干区域（Area），其中标准区域的特点是 （64） ；存根区域（stub）的特点是 （65） 。

（64）A．不接受本地 AS 之外的路由信息，也不接受其他区域的路由汇总信息

B．不接受本地 AS 之外的路由信息，对本地 AS 之外的目标采用默认路由

C．可以接收任何链路更新信息和路由汇总信息

D．可以学习其他 AS 的路由信息，对本地 AS 中的其他区域采用默认路由

（65）A．不接受本地 AS 之外的路由信息，也不接受其他区域的路由汇总信息

B．不接受本地 AS 之外的路由信息，对本地 AS 之外的目标采用默认路由

C．可以接收任何链路更新信息和路由汇总信息

D．可以学习其他 AS 的路由信息，对本地 AS 中的其他区域使用默认路由

**试题（64）、（65）分析**

为了适应大型网络配置的需要，OSPF 协议引入了“分层路由”的概念。如果网络规模很大，则路由器要学习的路由信息很多，对网络资源的消耗很大，所以典型的链路状态协议都把网络划分成较小的区域（Area），从而限制了路由信息传播的范围。每个区域就如同一个独立的网络，区域内的路由器只保存该区域的链路状态信息，使得路由器的链路状态数据库可以保持合理的大小，路由计算的时间和报文数量都不会太大。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

- 标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。
- 主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。
- 存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。
- 完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。
- 不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（64）C （65）B

**试题（66）、（67）**

NAT 技术解决了 IPv4 地址短缺的问题。假设内网的地址数是 m，而外网的地址数 n，若 m>n，则这种技术叫作__（66）__，若 m>n，且 n=1，则这种技术叫作__（67）__。

（66）A. 动态地址翻译 B. 静态地址翻译
C. 地址伪装 D. 地址变换

（67）A. 动态地址翻译 B. 静态地址翻译
C. 地址伪装 D. 地址变换

**试题（66）、（67）分析**

NAT 技术主要解决 IP 地址短缺问题，最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。局部地址是在子网内部独立编址的，可以与外部地址重叠。后来根据这种技术又开发出两种最主要的应用。

第一种应用是动态地址翻译（Dynamic Address Translation）。假定：

- m：需要翻译的内部地址数。
- n：可用的全局地址数（NAT 地址）。

当 m:n 翻译满足条件（m≥1 and m≥n）时，可以把一个大的地址空间映像到一个小的地址空间。所有 NAT 地址放在一个缓冲区中，并在存根域的边界路由器中建立一个局部地址和全局地址的动态映像表。这种 NAT 地址重用有如下特点：只要缓冲区中存在尚未使用的全局地址，任何从内向外的连接请求都可以得到响应，并且在边界路由器的动态 NAT 表为之建立一个映像表项；如果内部主机的映像存在，就可以利用它建立连接；从外部访问内部主机是有条件的，即动态 NAT 表中必须存在该主机的映像。

另外一种特殊的 NAT 应用是 m:1 翻译，这种技术也叫作伪装（masquerading），因为用一个路由器的 IP 地址可以把子网中所有主机的 IP 地址都隐蔽起来。如果子网中有多个主机同时都要通信，那么还要对端口号进行翻译，所以这种技术更经常被称为网络地址和端口翻译（Network Address Port Translation，NAPT）。在很多 NAPT 实现中专门保留一部分端口号给伪装使用，叫作伪装端口号。这种方法有如下特点。

① 出口分组的源地址被路由器的外部 IP 地址所代替，出口分组的源端口号被一个未使用的伪装端口号所代替。

② 如果进来的分组的目标地址是本地路由器的 IP 地址，而目标端口号是路由器的伪装端口号，则 NAT 路由器就检查该分组是否为当前的一个伪装会话，并试图通过伪装表对 IP 地址和端口号进行翻译。

伪装技术可以作为一种安全手段使用，借以限制外部网络对内部主机的访问。另外，还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。

**参考答案**

（66）A　（67）C

**试题（68）、（69）**

CIDR 技术解决了路由缩放问题。例如 2048 个 C 类网络组成一个地址块，网络号从 192.24.0.0～192.31.255.0，这样的超网号应为__（68）__，其地址掩码应为__（69）__。

（68）A．192.24.0.0　　B．192.31.255.0
　　C．192.31.0.0　　D．192.24.255.0

（69）A．255.255.248.0　　B．255.255.255.0
　　C．255.255.0.0　　D．255．248．0.0

**试题（68）、（69）分析**

2048 个 C 类网络 192.24.0.0～192.31.255.0 组成的超网号应为 192.24.0.0/13。

**参考答案**

（68）A　（69）D

**试题（70）**

网络系统设计过程中，物理网络设计阶段的任务是__（70）__。

（70）A．依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境
　　B．分析现有网络和新网络的各类资源分布，掌握网络所处的状态
　　C．根据需求规范和通信规范，实施资源分配和安全规划
　　D．理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

**试题（70）分析**

网络开发过程的五阶段迭代周期模型可以用下图来描述。

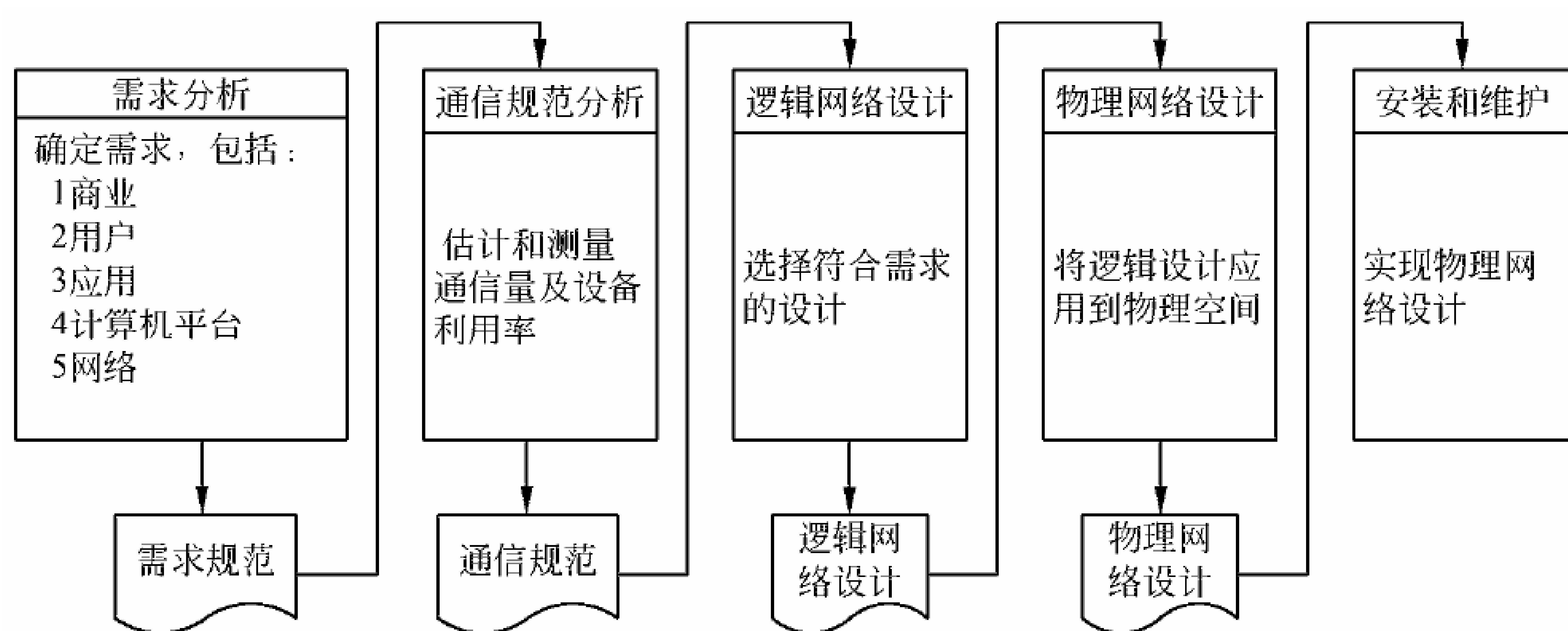



图　五阶段网络开发过程

① 需求分析。

需求分析是开发过程中最关键的阶段。通过和不同的用户（包括经理人员和网络管理员）交流，收集明确的需求信息。需求分析的输出是产生一份需求说明书，也就是需求规范。

② 现有网络系统的分析。

如果当前的网络开发过程是对现有网络的升级和改造，就必须进行现有网络系统的分析工作。现有网络系统分析的目的是描述资源分布，以便于在升级时尽量保护已有的投资。在这一阶段，应给出一份正式的通信规范说明文档，作为下一个阶段的输入。

③ 确定网络逻辑结构。

网络逻辑结构设计是根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。这个阶段最后应该得到一份逻辑设计文档。

④ 确定网络物理结构。

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。

⑤ 安装和维护。

这个阶段是根据前面的工程成果实施环境准备、设备安装调试的过程。网络安装完成网络投入运行后，还需要做大量的故障监测和故障恢复，以及网络升级和性能优化等维护工作。

**参考答案**

（70）A

**试题（71）～（75）**

The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is to chop up its __（71）__ by using one of the multiplexing schemes, such as FDM. If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion. Since each user has a private frequency __（72）__, there is now no interference among users. When there is only a small and constant number of users, each of which has a steady stream or a heavy load of __（73）__, this division is a simple and efficient allocation mechanism. A wireless example is FM radio stations. Each station gets a portion of the FM band and uses it most of the time to broadcast its signal. However, when the number of senders is large and varying or the traffic is __（74）__, FDM presents some problems. If the spectrum is cut up into N regions and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted. And if more than N users want to communicate, some of them will be denied __（75）__ for lack of bandwidth, even if some of the users who have been assigned a frequency band hardly ever transmit or receive anything.

（71）A．capability　B．capacity　C．ability　D．power
（72）A．band　B．range　C．domain　D．assignment
（73）A．traffic　B．data　C．information　D．communications
（74）A．continuous　B．steady　C．bursty　D．flow
（75）A．allowance　B．connection　C．percussion　D．permission

**参考译文**

在多个竞争的用户之间分配单一信道（例如电话干线）的传统方法就是通过一种多路方案（例如 FDM）将其带宽分解开来。如果有 N 个用户，带宽就被分成 N 个相等的部分，每一个用户都得到了自己的一份。因为每个用户都有一个专用的频带，所以用户之间没有干扰。当仅有少量的、固定数量的用户，而且每个用户都有一个稳定的流量或者大量的通信负载时，这种划分才是简单而有效的分配机制。无线通信中的 FM 广播系统就是这样的例子。每一个广播台都得到一部分 FM 频带，并使用这个频带经常性地进行无线广播。然而，当发送者的数量是大量的、变化的或者突发式通信时，FDM 就会出问题。如果频谱被分成 N 个部分，而且划分的数量少于需要通信的用户数量时，一大片有价值的频谱就会被浪费。如果超过 N 个用户需要通信，某些用户就会因没有带宽而被拒绝进入连接，即使某些用户曾经被赋予频带，发送或接收过一些信息。

**参考答案**

（71）B　（72）A　（73）A　（74）C　（75）D

# 第 22 章　2014 上半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位计划部署园区网络，该单位总部设在 A 区，另有两个分部分别设在 B 区和 C 区，各个地区之间的距离分布如图 1-1 所示。

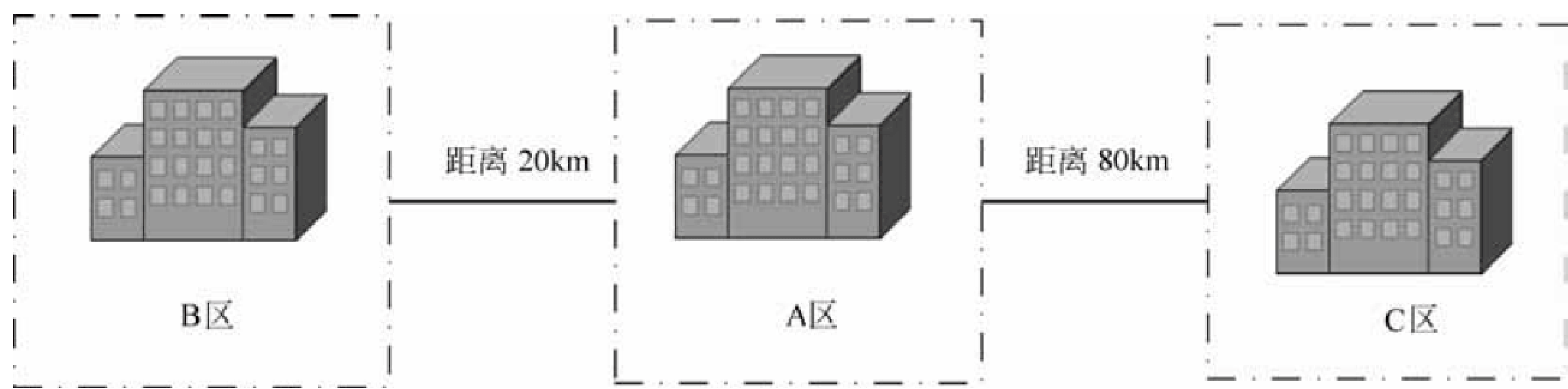



图 1-1

该单位的主要网络业务需求在 A 区，网络中心及服务器机房亦部署在 A 区；B 区的网络业务流量需求远大于 C 区；C 区虽然业务量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互联互通并且都能访问互联网。同时基于安全考虑，该单位要求采用一套认证设备进行身份认证和上网行为管理。

**【问题 1】（6 分）**

为保障业务需求，该单位采用两家运营商接入 Internet。根据题目需求，回答以下问题：

1．两家运营商的 Internet 接入线路应部署在哪个区？为什么？

2．网络运营商提供了 MPLS VPN 和千兆裸光纤两种互联方式，哪一种可靠性高？为什么？

3．综合考虑网络需求及运行成本，AB 区之间与 AC 区之间分别采用上述哪种方式进行互联？

**【问题 2】（8 分）**

该单位网络部署接入点情况如表 1-1 所示。

表 1-1

| 区　域 | 汇　聚　点 | 接　入　点 | 备　注 |
|---|---|---|---|
| A | 办公楼 | 124 | 所有区域采用三层局域网结构部署，其中 A 区采用双核心交换机冗余。所有汇聚点采用单模光纤上联至核心交换机。所有接入交换机采用双绞线上联至汇聚交换机 |
| | 资料室 | 86 | |
| | 网管中心 | 78 | |
| | 设计中心 | 200 | |
| | 生产区 | 115 | |
| B | 办公楼 | 106 | |
| | 培训中心 | 126 | |
| | 宿舍 | 198 | |
| C | 办公楼 | 86 | |
| | 营销中心 | 54 | |

根据网络部署需求，该单位采购了相应的网络设备，请根据题目说明及表 1-1，确定表 1-2 所示的设备数量及合理的部署位置（注：不考虑双绞线的距离限制）。

表 1-2

| 设 备 类 型 | 设 备 数 量 | 部 署 区 域 |
|---|---|---|
| 核心交换机 | （1） | A 区 |
| 核心交换机 | 1 | B 区 |
| 核心交换机 | 1 | C 区 |
| 汇聚交换机 | 5 | A 区 |
| 汇聚交换机 | 3 | B 区 |
| 汇聚交换机 | 2 | C 区 |
| SFP 单模模块 | 5 | （2）区 |
| SFP 单模模块 | 7 | （3）区 |
| SFP 单模模块 | 22 | （4）区 |
| 24 口接入交换机 | （5） | A 区 |
| 24 口接入交换机 | （6） | B 区 |
| 24 口接入交换机 | （7） | C 区 |
| 千兆服务器接入交换机 | 1 | A 区 |
| 服务器 | 3 | A 区 |
| 路由器 | 1 | （8）区 |
| 认证及流控设备 | 1 | A 区 |
| 防火墙 | 1 | A 区 |

**【问题 3】（6 分）**

根据题目要求，在图 1-2 的方框中画出该单位的 A 区网络拓扑示意图（汇聚层以下不画）。

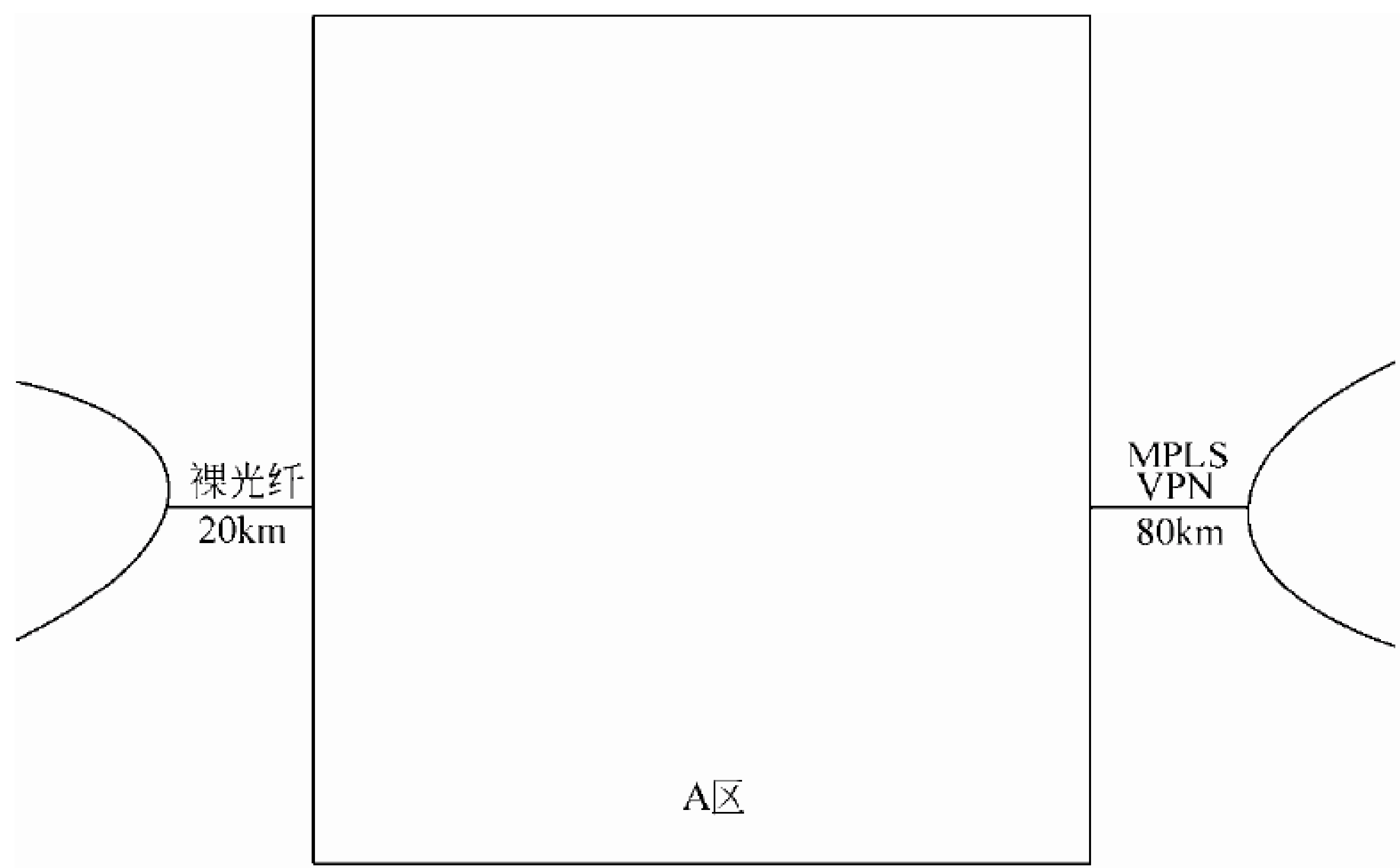



图 1-2

**试题一分析**

本题考查的是网络规划的基本知识。

**【问题 1】**

本问题考查广域网接入及网络互联的问题。

1．两家运营商的 Internet 接入线路应部署在 A 区。其主要原因有两点：首先，根据题目描述该单位的主要网络业务需求在 A 区，网络中心及服务器机房亦部署在 A 区，另外，该单位要求采用一套认证设备进行身份认证和上网行为管理，所以出口线路应集中在一个业务需求大的区域（A 区）。这时，由于三个区域是互通的，其他区域也可通过 A 区出口与互联网连接。

2．网络运营商提供了 MPLS VPN 和千兆裸光纤两种互联方式。这两种互联方式中 MPLS VPN 的可靠性大于千兆裸光纤，这是由于当千兆裸光纤是物理链路，当其出现链路故障时，互联业务就会中断。MPLS VPN 属于逻辑链路。当单个物理链路出现故障时，只要其他链路可达，MPLS VPN 还可提供互联服务。

3．综合考虑网络需求及运行成本，AB 区之间应采取千兆裸光纤互联模式，AC 区之间应采用 MPLS VPN 互联方式。

根据题目描述，B 区的网络业务流量需求远大于 C 区；C 区虽然业务量小，但是网络可靠性要求高。所以，AB 区之间采取千兆裸光纤以适应大业务量，AC 区之间采用 MPLS VPN 在业务量不大但安全性要求较高时是合理的。

**【问题 2】**

本问题考查的是网络设备选型的基础知识。

1．根据题目描述可知，A 区采用双核心交换机冗余，所以 A 区核心交换机的数量为 2 台。

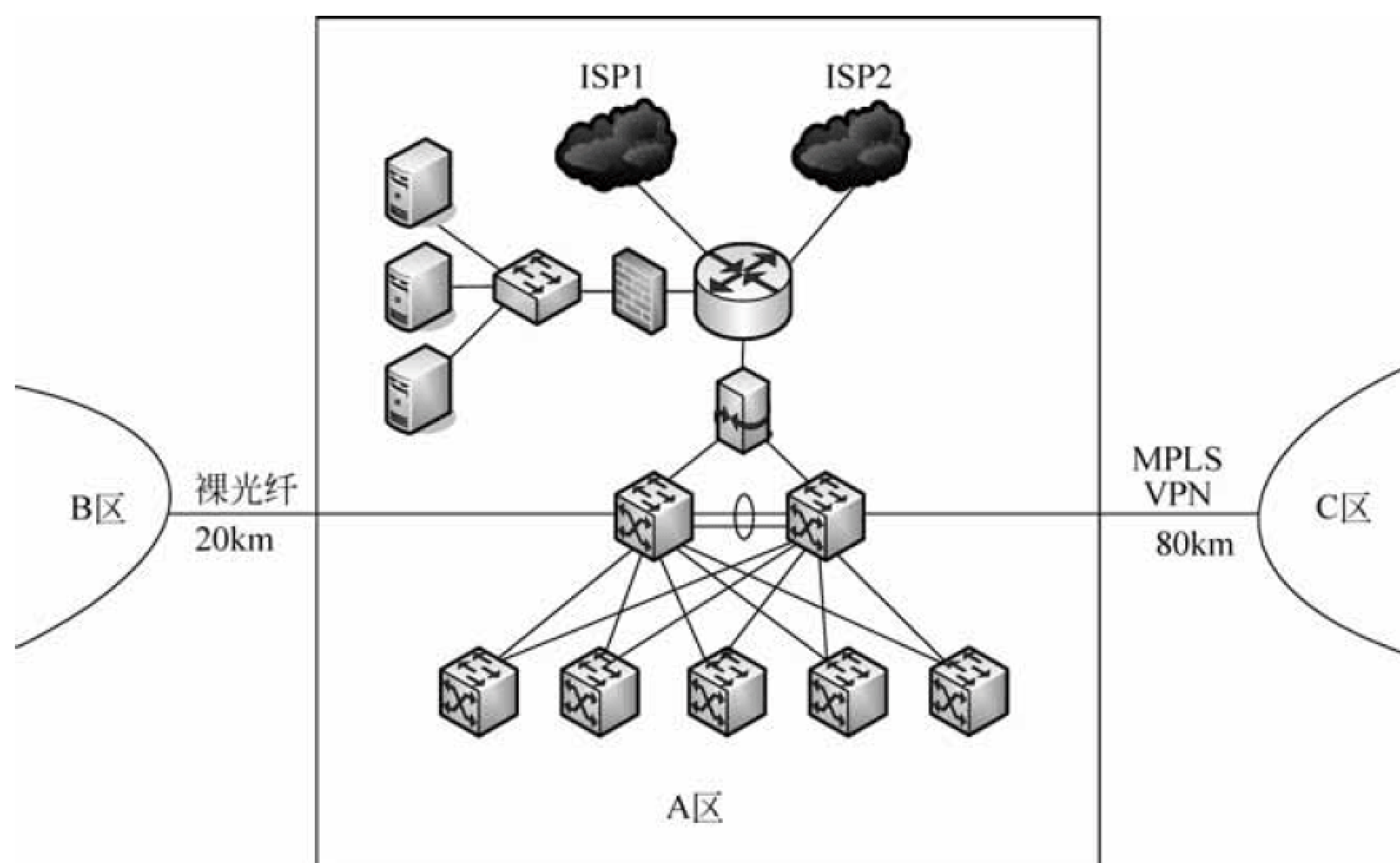
2．根据题目描述可知，所有汇聚点采用单模光纤上联至核心交换机 SFP 单模模块。A、B、C 区的汇聚交换机分别有 5、3、2 台，其中 A 区是双核心交换机，故核心与汇聚相连需要 20 个 SFP 单模模块，另外 A 区需要和 B、C 区核心交换机互联，所以还需要 2 个 SFP 单模模块，共计 22 个。同样可以推算出 B 区需要 7 个 SFP 单模模块，C 区需要 5 个 SFP 单模模块。

3．A、B、C 区的接入点数参见表 1-1，不考虑双绞线的距离限制，只需要计算同一个楼内需要的 24 口接入交换机数量即可。根据计算可知，A 区需要 24 口接入交换机 28 个，B 区需要 24 口接入交换机 20 个，C 区需要 24 口接入交换机 7 个。

4．由前述可知，Internet 接入线路部署在 A 区，所以路由器应部署在 A 区。

**【问题 3】**

本问题考查的是网络拓扑的基础知识。根据题目的描述和设备配置表，注意 A 区双核心的链路冗余的情况，另外注意 B 区和 C 区与 A 区互联分别采用裸光纤和 MPLS VPN，所以网络拓扑结构图如下。




## 参考答案

**【问题 1】**

1．部署在 A 区。网络业务主体在 A 区，采用一套认证和上网行为管理。

2．MPLS VPN 可靠性比较高，线路有冗余。

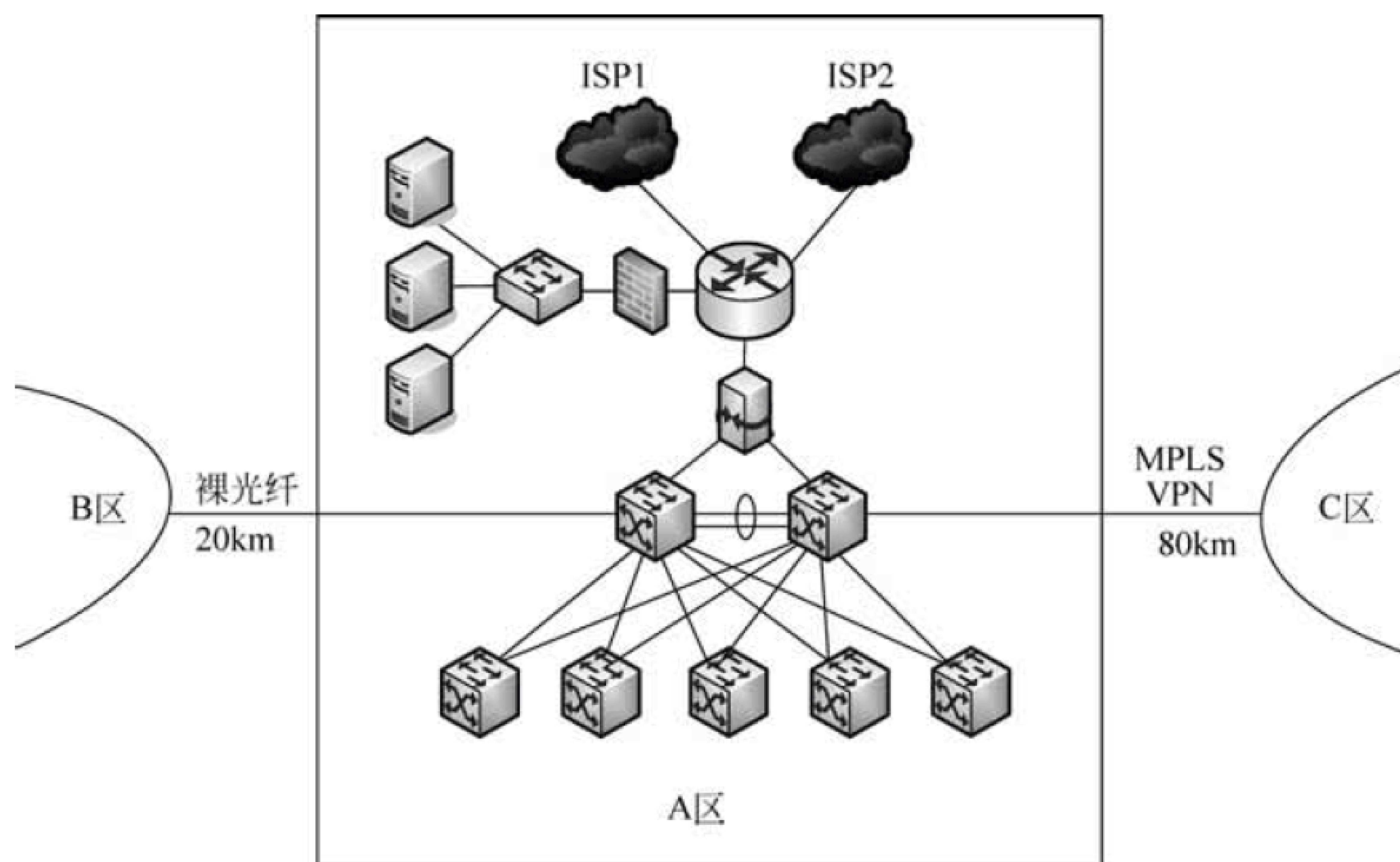
3．AB 区之间采用千兆裸光纤， AC 区之间采用 MPLS VPN。

**【问题 2】**

（1）2 （2）C （3）B （4）A

（5）28 （6）20 （7）7 （8）A

【问题 3】




试题二（共 15 分）

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某公司采用 Windows Server 2003 操作系统搭建该公司的企业网站，要求用户在浏览器地址栏必须输入 https://www.gongsi.com/index.html 或 https://117.112.89.67/index.html 来访问该公司网站。其中，index.html 文件存放在网站所在服务器 E:\gsdata 目录中。在服务器上安装完成 IIS 6.0 后，网站的属性窗口【网站】、【主目录】选项卡分别如图 2-1 和图 2-2 所示。

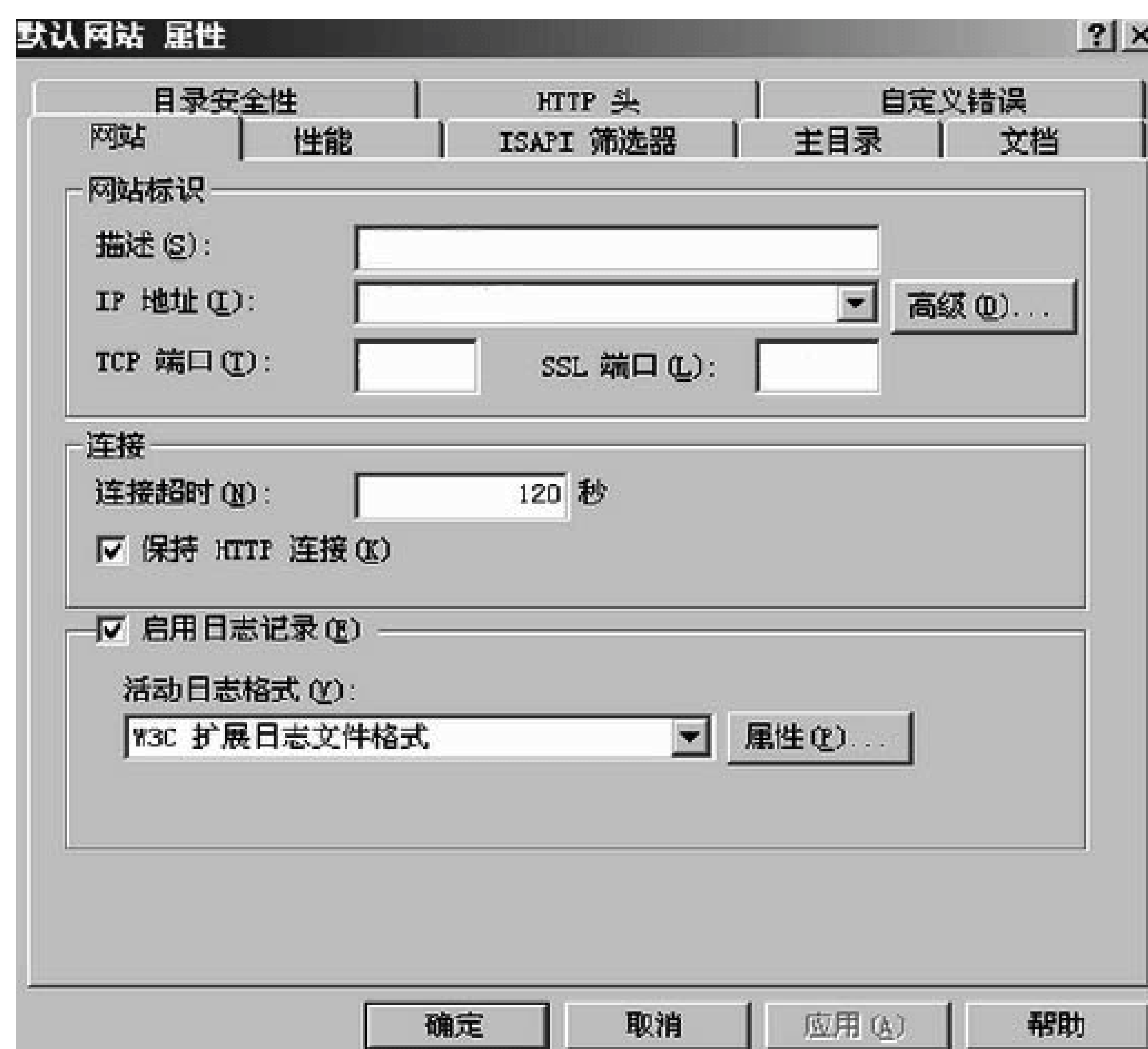



图 2-1

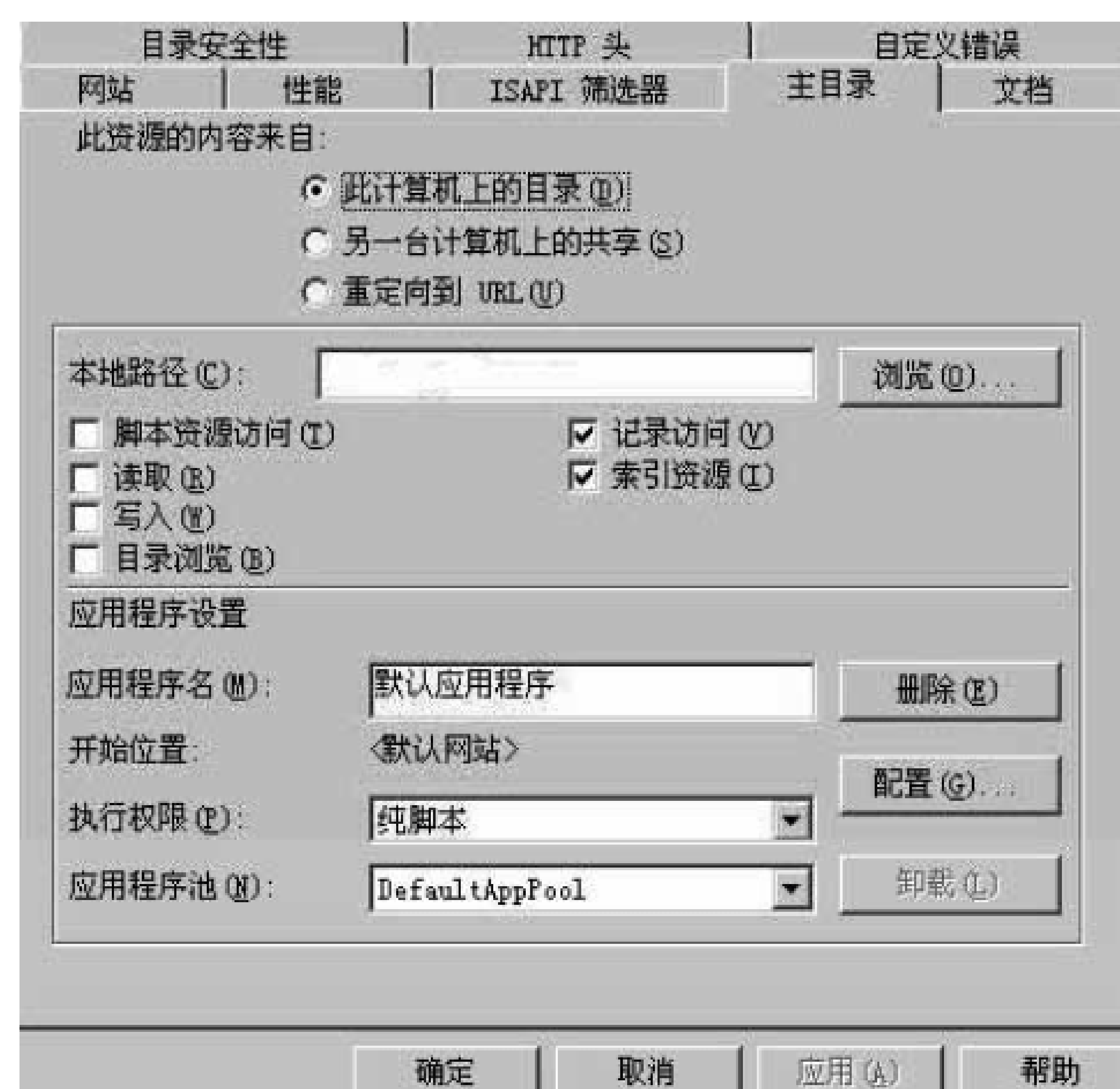



图 2-2

【问题 1】（4 分）

1．按照题目说明，图 2-1 中的“IP 地址”文本框中的内容应为＿＿（1）＿＿；“SSL 端口”文本框中的内容应为＿＿（2）＿＿。

2．在图 2-2 中，“本地路径”文本框中的内容应为＿＿（3）＿＿；同时要保障用户通过题目要求的方式来访问网站，必须至少勾选＿＿（4）＿＿复选框。

（4）备选答案：

A．脚本资源访问　　B．读取　　C．写入　　D．目录浏览

【问题 2】（6 分）

1．配置该网站时，需要在如图 2-3 所示的【目录安全性】选项卡中单击【服务器证书】按钮来获取服务器证书。其中获取服务器证书的步骤顺序如下：① 生成证书请求文件；② ＿＿（5）＿＿；③从 CA 导出证书文件；④在 IIS 服务器上导入并安装证书。

配置完成后，当用户登录该网站时，通过验证 CA 的签名来确认该数字证书的有效性，从而＿＿（6）＿＿，CA 颁发给 Web 网站的数字证书中不包括＿＿（7）＿＿。

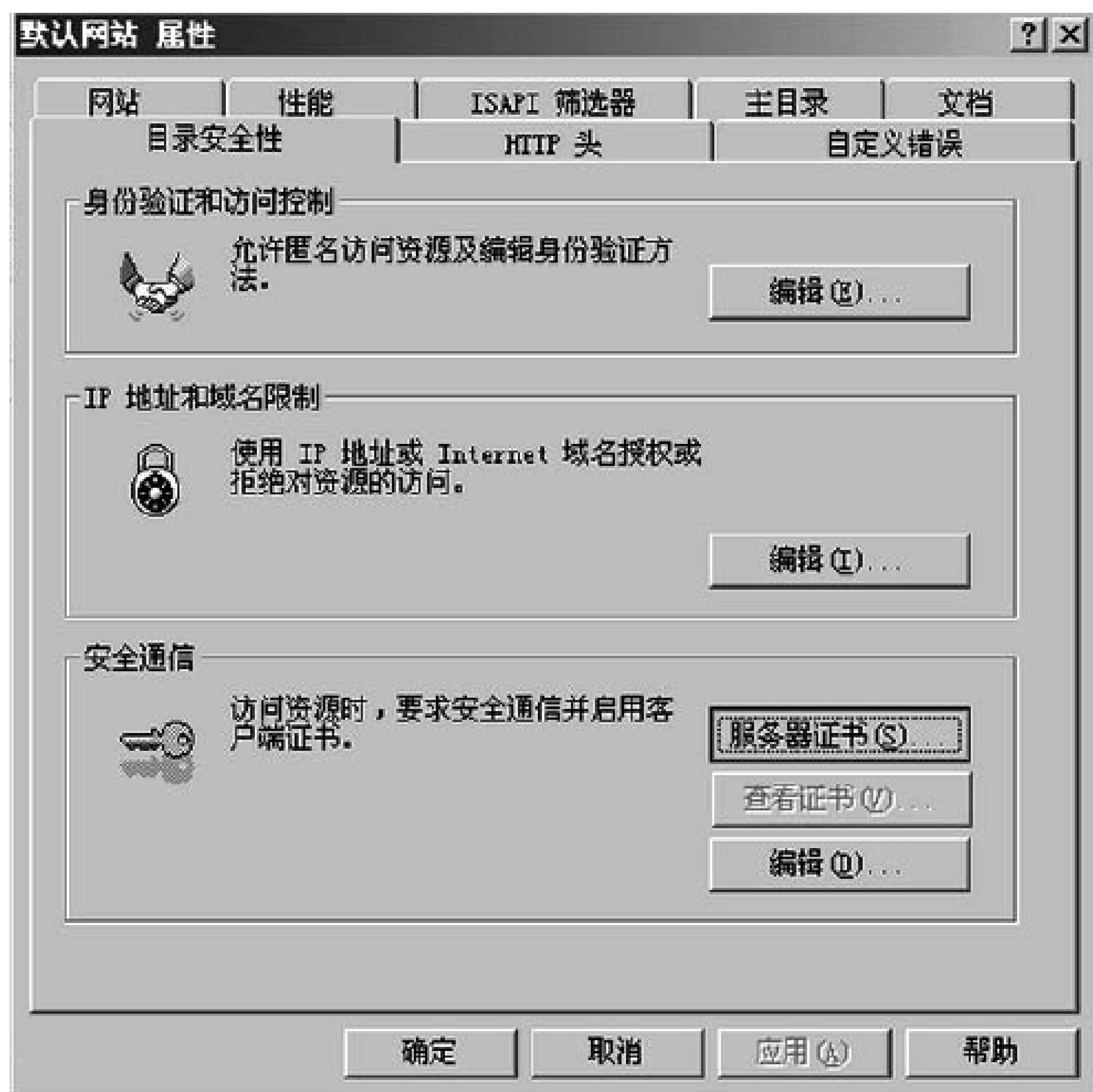



图 2-3

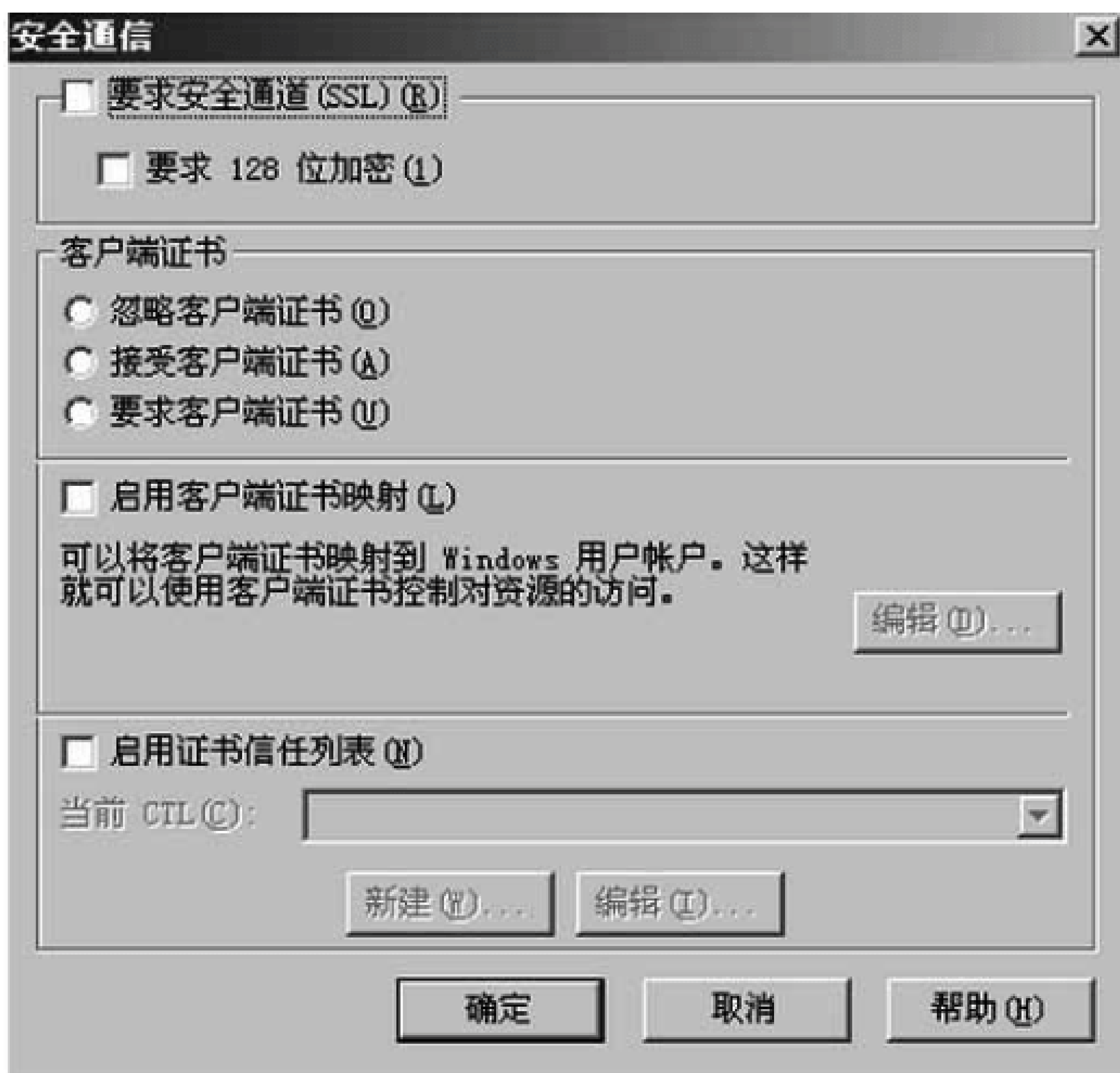



图 2-4

（6）、（7）备选答案：

（6）A．验证网站的真伪　　B．判断用户的权限

C．加密发往服务器的数据　　D．解密所接受的客户端数据

（7）A．证书的有效期　　B．网站的公钥

C．证书的序列号　　D．网站的私钥

【问题 3】（2 分）

配置该网站时，在图 2-3 所示的窗口中单击【安全通信】栏目中的【编辑】按钮，弹出如图 2-4 所示的窗口。按照题目要求，客户端浏览器只能通过 HTTPS 方式访问服务

器，此时应勾选图 2-4 中的___（8）___框。如果要求客户端和服务器进行双向认证，此时应该勾选图 2-4 中的___（9）___框。

**【问题 4】（2 分）**

HTTPS 用于在客户计算机和服务器之间提供安全通信，广泛用于因特网上安全敏感的应用，例如___（10）___应用。

HTTPS 使用安全套接字层（SSL）进行信息交换。SSL 目前的版本是 3.0，被 IETF 定义在 RFC 6101 中。IETF 对 SSL 进行升级后的继任者是___（11）___。

（10）备选答案：

A．网络聊天　　B．网络视频　　C．网上交易　　D．网络下载

**【问题 5】（1 分）**

使用 HTTPS 能不能确保服务器自身的安全？

**试题二分析**

本题考查的是利用 Windows Server 2003 操作系统搭建安全的 Web 网站的相关知识。

**【问题 1】**

本问题主要考查的是利用 IIS 搭建 web 站点的配置过程。

在图 2-1 可从“IP 地址”下拉框中指定一个 IP 地址或者输入用于访问该站点的 IP 地址。如果没有分配指定的 IP 地址，即选中“全部未分配”选项，那么此站点将响应分配给该服务器但没有分配给其他站点的所有 IP 地址，并使它成为默认网站的 IP 地址。“SSL 端口”文本框是可选项目，用于指派与该网站标识相关联的 SSL 端口。默认的 SSL 端口号是 443。只有使用 SSL 加密时才需要 SSL 端口号。题目要求用户在浏览器地址栏必须输入 https://www.gongsi.com/index.html 或 https://117.112.89.67/index.html 来访问该公司网站。所以在图 2-1 中的“IP 地址”文本框中的内容应为 117.112.89.67 或者全部未分配，“SSL 端口”文本框中的内容应为 443。

另外，根据题目要求 index.html 文件存放在网站所在服务器 E:\gsdata 目录中。所以在图 2-2 中所示的“主目录”选项卡中“本地路径”文本框中的内容应为“E:\gsdata”，以指明网站首页文档的物理存放路径。为保障用户对网站的访问，在图 2-2 中应该至少勾选“读取”复选框，并单击“确定”或者“应用”按钮。

**【问题 2】**

本问题主要考查的是配置安全的 Web 网站时的步骤。

为了配置安全的 Web 网站，获取并安装服务器证书的步骤依次为：① 从“管理工具”中进入“Internet 服务管理器”，右击需要配置的站点，在弹出的快捷菜单中选择“属性”命令，接着单击“目录安全性”选项卡中的“安全通信”组件框中“服务器证书”按钮，通过 IIS 证书向导生成证书请求文件。② 向证书颁发机构（CA）提交证书请求文件，证书颁发机构颁发相应的证书。③ 在申请证书的计算机浏览器上输入 http://根 CA 的 IP/certsrv，进入证书申请页面。单击“检查挂起的证书”链接，选择已经提交的

证书申请。如果颁发机构已将证书颁发，则可单击“安装此证书”按钮，即从证书颁发机构导出证书文件。④ 在“目录安全性”选项卡中再次单击“安全通信”组件框中的“服务器证书”按钮。在 IIS 证书向导中进入“挂起的证书请求”页面，选择“处理挂起的请求，并安装证书”单选按钮，接着选择刚才导出的 CER 文件。完成在 IIS 服务器上导入并安装证书。⑤ 在“目录安全性”选项卡中单击“安全通信”组件框中的“编辑”按钮，打开“安全通信”对话框。在该对话框中可根据所需要的安全要求配置相应的身份验证方式和 SSL 安全通道。

综上所述，为配置安全的 Web 网站，获取并安装服务器证书的步骤顺序如下：①生成证书请求文件；②CA 颁发证书；③从 CA 导出证书文件；④在 IIS 服务器上导入并安装证书。

数字证书能够验证一个实体身份，而这是在保证数字证书本身有效性的前提下才能够实现的。验证数字证书的有效性是通过验证 CA 的签名实现的。某网站向 CA 申请了数字证书，当用户登录该网站时通过验证 CA 对其的签名来确认该数字证书的有效性，从而验证该网站的真伪。CA 颁发给网站的数字证书包含多项内容（如证书的版本号、序列号、网站的公钥、CA 的签名、证书的有效期等），但是不包括网站的私钥。

**【问题 3】**

本问题主要考查配置安全的 Web 网站的过程。

配置安全的 Web 站点时，在图 2-3 中的“目录安全性”选项卡中单击“安全通信”组件框中的“编辑”按钮，系统将打开图 2-4 中“安全通信”对话框。如果要求客户只能通过使用 HTTPS 服务访问该网站，则应该选中“要求安全通道（SSL）”复选框。

在“客户端证书”下，选择以下某一选项以启用客户端证书验证：接受客户端证书，用户可以使用客户端证书访问资源，但证书并不必需。若要求客户端证书，则服务器在将用户与资源连接之前要请求客户端证书，将拒绝没有有效客户端证书的用户的访问。若忽略客户端证书，无论用户是否拥有证书，都将被授予访问权限。如果要求客户端和服务器进行双向认证，则应该选中“要求客户端证书”复选框。

**【问题 4】**

本问题主要考查的是 HTTPS 的基本知识。

Https 是基于安全目的的 Http 通道，其安全基础由 SSL 层来保证。最初由 netscape 公司研发，主要提供了通讯双方的身份认证和加密通信方法。现在广泛应用于互联网上对安全敏感的通讯，如网上交易、在线支付等。

安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出 Web 浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL 在传输层对网络连接进行加密。

SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。它在服务器和客户机两端可同时被支持，目前已成为

互联网上保密通讯的工业标准。现行 Web 浏览器亦普遍将 HTTP 和 SSL 相结合，从而实现安全通信。此协议的继任者是 TLS。

IETF（www.ietf.org）将 SSL 作了标准化，即 RFC2246，并将其称为 TLS（Transport Layer Security），其最新版本是 RFC5246,版本 1.2。从技术上讲，TLS1.0 与 SSL3.0 的差异非常微小。TLS 利用密钥算法在互联网上提供端点身份认证与通讯保密，其基础是公钥基础设施（public key infrastructure，PKI）。

**【问题 5】**

Https 的限制主要是它的安全保护依赖浏览器的正确实现以及服务器软件、实际加密算法的支持。这里面一种常见的误解是“银行用户在线使用 https:就能充分彻底保障他们的银行卡号不被偷窃。”实际上，与服务器的加密连接中能保护银行卡号的部分，只有用户到服务器之间的连接及服务器自身。并不能绝对确保服务器自己是安全的，这点甚至已被攻击者利用，常见例子是模仿银行域名的钓鱼攻击。少数罕见攻击在网站传输客户数据时发生，攻击者尝试窃听数据于传输中。商业网站被人们期望迅速尽早引入新的特殊处理程序到金融网关，仅保留传输码（transaction number）。不过他们常常存储银行卡号在同一个数据库里。那些数据库和服务器少数情况有可能被未授权用户攻击和损害。因此使用 HTTPS 不能确保服务器自身的安全。

**参考答案**

**【问题 1】**

（1）117.112.89.67 或者 全部未分配

（2）443

（3）E:\gsdata

（4）B

**【问题 2】**

（5）CA 颁发证书

（6）A

（7）D

**【问题 3】**

（8）要求安全通道（SSL）

（9）要求客户端证书

**【问题 4】**

（10）C

（11）TLS 或者 Transport Layer Security

**【问题 5】**

不能

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某单位网络拓扑结构如图 3-1 所示，在 Linux 系统下构建 DNS 服务器、DHCP 服务器和 Web 服务器，要求如下：

1．路由器连接各个子网的接口信息如下：

（1）路由器 E0 口的 IP 地址为 192.168.1.1/25；

（2）路由器 E1 口的 IP 地址为 192.168.1.129/25；

（3）路由器 E2 口的 IP 地址为 192.168.2.1/29；

（4）路由器 E3 口的 IP 地址为 192.168.2.33/29。

2．子网 1 和子网 2 内的客户机通过 DHCP 服务器动态分配 IP 地址；

3．服务器设置固定 IP 地址，其中：

（1）DNS 服务器采用 BIND 构建，IP 地址为 192.168.2.2；

（2）DHCP 服务器 IP 地址为 192.168.2.3；

（3）Web 服务器网卡 eth0 的 IP 地址为 192.168.2.4， eth1 的 IP 地址为 192.168.2.34。

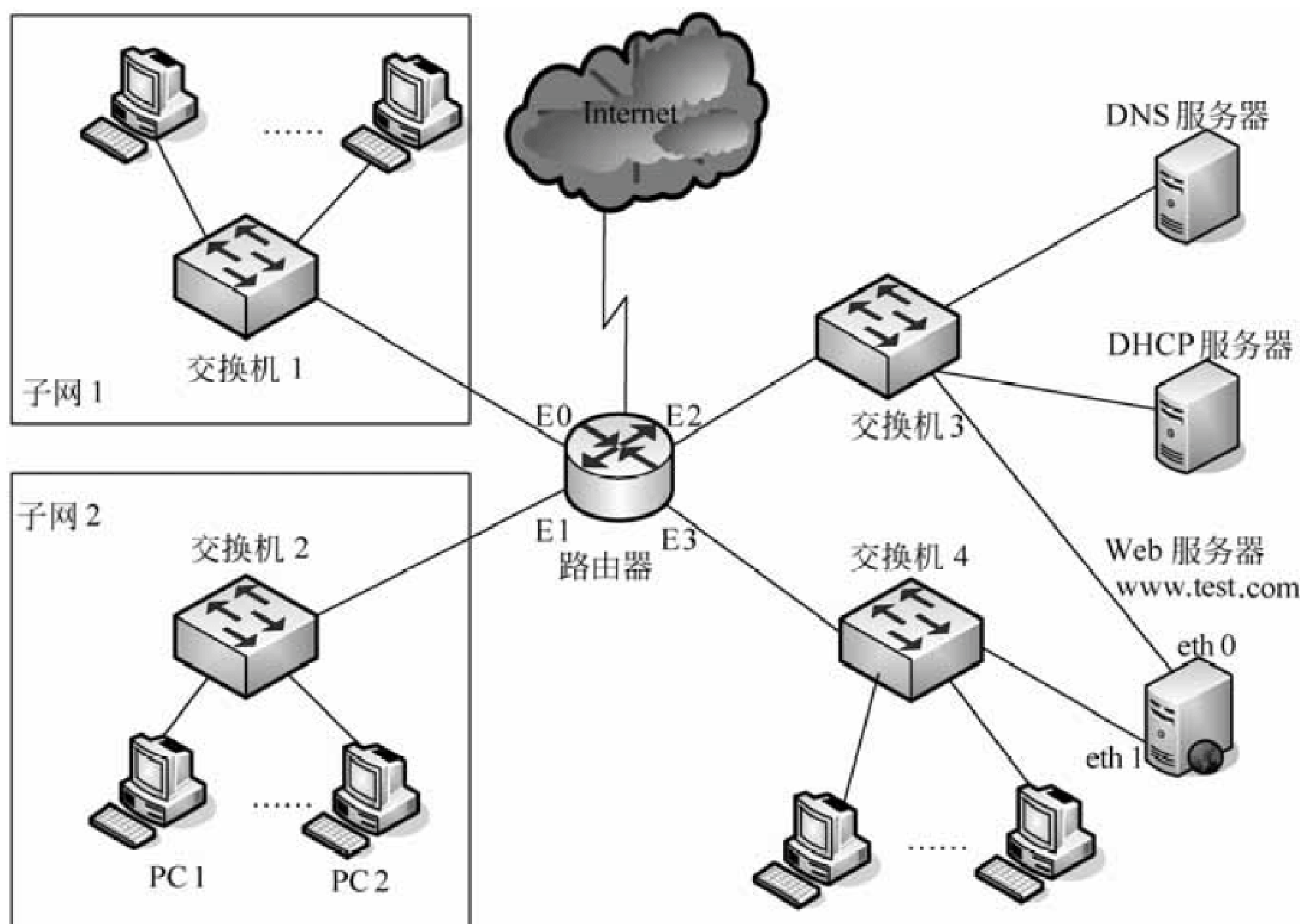



图 3-1

**【问题 1】（3 分）**

请完成图 3-1 中 Web 服务器 eth1 的配置。

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:24:F8:9B
NETMASK=___(1)___
IPADDR=___(2)___
GATEWAY=___(3)___
TYPE=Ethernet
NAME="System eth1"
IPV6INIT=no
```

**【问题 2】（3 分）**

请完成图 3-1 中 DNS 服务器网卡的配置。

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
HWADDR=08:00:27:21:A1:78
NETMASK=___(4)___
IPADDR=___(5)___
GATEWAY=___(6)___
TYPE=Ethernet
NAME="System eth0"
IPV6INIT=no
```

**【问题 3】（6 分）**

请在（7）、（8）、（9）处填写恰当的内容。

在 Linux 系统中设置域名解析服务器，已知该域名服务器上文件 named.conf 的部分内容如下：

```
options {
    directory "/var/named";
    hostname    "ns1.test.com";
    allow-query {any;};
    allow-recursion {A;B;C;D};
    recursion yes;
    };
acl "A" { 192.168.1.0/25;};
acl "B" { 192.168.1.128/25;};
acl "C" { 192.168.2.0/29;};
```

```
acl "D" { 192.168.2.32/29;};
view "A " {
   match-clients { A; };
   recursion yes;
   zone "test.com" {
   type master;
   file "test.com.zone.A"
   };
   };
view "B" {
   match-clients { any; };
   recursion yes;
   zone "test.com" {
   type master;
   file "test.com.zone.B"
   };
   };
```

test.com.zone.A 文件的部分配置如下：www　IN　A　192.168.2.4

test.com.zone.B 文件的部分配置如下：www　IN　A　192.168.2.34

IP 地址__（7）__不允许使用该 DNS 进行递归查询，子网 1 和子网 2 中的客户端访问 www.test.com 时，该 DNS 解析返回的 IP 地址分别为__（8）__和__（9）__。

（7）备选答案：

A．192.168.1.8　　B．192.168.1.133

C．192.168.2.10　　D．192.168.2.6

（8）、（9）备选答案：

A．192.168.2.4　　B．192.168.2.34

C．192.168.2.4 或者 192.168.2.34　　D．192.168.2.3 和 192.168.2.34

**【问题 4】（8 分）**

DHCP 服务器配置文件如下所示：

```
authoritative;
ddns-updates off;
max-lease-time 604800;
default-lease-time 604800;
allow unknown-clients;
option domain-name-servers 192.168.2.2
ddns-update-style none;
allow client-updates;
```

```
subnet 192.168.2.32 netmask 255.255.255.248 {
    option routers 192.168.2.33;
    range 192.168.2.35 192.168.2.38;
}
```

根据这个文件中的内容，该 DHCP 服务的默认租期是__（10）__天，DHCP 客户机能获得的 IP 地址范围是：从__（11）__到__（12）__，获得的 DNS 服务器 IP 地址为__（13）__。

**试题三分析**

本题考查网络地址子网掩码计算、Linux 系统下网络配置、DNS 服务配置和 DHCP 服务配置方面的知识。

**【问题 1】**

本问题考查网络地址规划和 Linux 系统下网卡网络配置的基本知识。

两种表示方式的子网掩码换算，29 位的子网掩码换算后为 255.255.255.248。

Linux 系统下网络配置参数中 NETMASK 代表子网掩码，IPADDR 代表 IP 地址，GATEWAY 代表子网网关地址。

**【问题 2】**

本问题考查网络地址规划和 Linux 系统下网卡网络配置的基本知识和两种表示方式的子网掩码换算。

Linux 系统下网络配置参数中 NETMASK 代表子网掩码，IPADDR 代表 IP 地址，GATEWAY 代表子网网关地址。

**【问题 3】**

本问题考查 Linux 系统下基于 BIND 的 DNS 服务配置。

通过 allow-recursion{A;B;C;D}命令，可以看出 acl A、B、C、D 允许递归查询，选项 A、B、D 对应的 IP 地址分别在定义的 acl A、B、C 子网中，选项 C 对应的 IP 地址不在 acl A、B、C、D 任何子网中，故选 C。

客户端访问 www.test.com 时，子网 1 的客户端对应 acl A，会访问 view A 中的域名配置文件 test.com.zone.A，故解析出的 IP 地址为 192.168.2.4；子网 2 的客户端不在 acl A 中，则会访问 view B 中的域名配置文件 test.com.zone.B，故解析出的 IP 地址为 192.168.2.34。

**【问题 4】**

本问题考查 Linux 系统下 DHCP 服务配置的基础知识。

配置文件中 default-lease-time 604800 代表 DHCP 服务器设置的默认租期为 604800 秒，转换成天数应为 7 天。

配置文件中 option routers 192.168.2.33 代表 DHCP 客户机的子网网关地址，range 192.168.2.35 192.168.2.38 代表 DHCP 客户机能获得的 IP 地址范围。

配置文件中 option domain-name-servers 192.168.2.2 代表 DNS 服务器 IP 地址为

192.168.2.2。

**参考答案**

**【问题 1】**

（1）255.255.255.248

（2）192.168.2.34

（3）192.168.2.33

**【问题 2】**

（4）255.255.255.248

（5）192.168.2.2

（6）192.168.2.1

**【问题 3】**

（7）C

（8）A

（9）B

**【问题 4】**

（10）7

（11）192.168.2.35

（12）192.168.2.38

（13）192.168.2.2

**试题四（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业总部设立在 A 地，在 B 地建有分支机构，分支机构和总部需要在网络上进行频繁的数据传输，该企业网络采用 IPSec VPN 虚拟专用网技术实现分支机构和总部之间安全、快捷、经济的跨区域网络连接。

该企业的网络拓扑结构如图 4-1 所示。

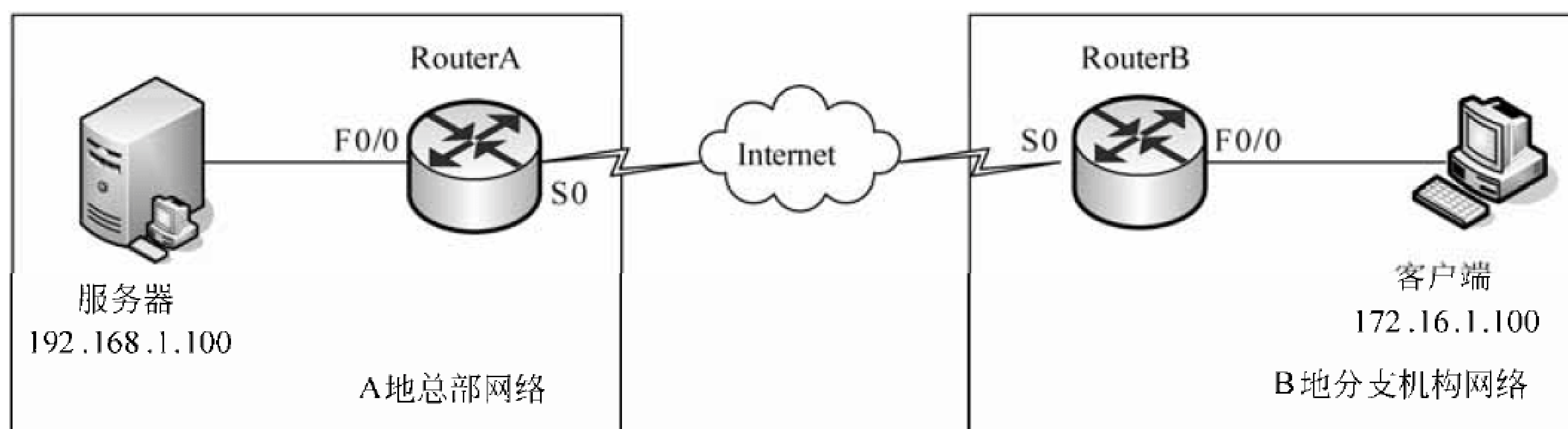



图 4-1

该企业的网络地址规划及配置如表 4-1 所示。

**表 4-1 网络规划地址配置表**

| 设　备 | IP 地址 | 设　备 | IP 地址 |
|---|---|---|---|
| RouterA | F0/0:192.168.1.1/24<br>S0:202.102.100.1/30 | RouterB | F0/0:172.16.1.1/24<br>S0:202.102.100.2/30 |
| 总部服务器 | 192.168.1.100/24 | 分支机构客户端 | 172.16.1.100/24 |

**【问题 1】（7 分）**

为了完成对 RouterA 和 RouterB 的远程连接管理，以 RouterA 为例，完成初始化路由器，并配置 RouterA 的远程管理地址（192.168.1.20），同时开启 RouterA 的 Telnet 功能并设置全局配置模式的访问密码，请补充完成下列配置命令。

```
RouterA >enable
RouterA#configure terminal
RouterA(config)#interface  f0/0         //进入 F0/0 的___(1)___子模式
RouterA(config-if)#ip addr ___(2)___   //为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut//___(3)___F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter ___(4)___     //进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr ___(5)___    //为 loopback 0 接口配置 IP 地址
......
RouterA(config)#___(6)___              //进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001 //配置 vty 口令为"abc001"
RouterA(config)#enable password abc001//配置全局配置模式的明文密码为"abc001"
RouterA(config)# enable___(7)___ abc001//配置全局配置模式的密文密码为"abc001"
......
```

**【问题 2】（5 分）**

VPN 是建立在两个局域网出口之间的隧道连接，所以两个 VPN 设备必须能够满足内网访问互联网的要求，以及需要配置 NAT。按照题目要求以 RouterA 为例，请补充完成下列配置命令。

```
RouterA(config)#access-list 101 ___(8)___ ip 192.168.1.0 0.0.0.255 172.16.1.0
0.0.0.255
RouterA(config)# access-list 101 ___(9)___ ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流
RouterA(config)#ip nat inside source list 101 interface ___(10)___ overload
//定义 NAT 转换关系
RouterA(config)#int ___(11)___
RouterA(config-if)#ip nat inside
RouterA(config)#int ___(12)___
```

```
RouterA(config-if)#ip nat outside    //定义 NAT 的内部和外部接口
......
```

**【问题 3】（4 分）**

配置 IPSec VPN 时要注意隧道两端的设备配置参数必须对应匹配，否则 VPN 配置将会失败。以 RouterB 为例配置 IPSec VPN，请完成相关配置命令。

```
RouterB(config)# access-list 102 permit ip ___(13)___
                                      //定义需要通过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp ___(14)___    //启用 ISAKMP(IKE)
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
RouterB(config-isakmp)#encryption des
RouterB(config-isakmp)#hash md5
RouterB(config-isakmp)#group 2
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address ___(15)___
                                     //指定共享密钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
RouterB(config)#crypto map abc001 10 ipsec-isakmp
......
RouterB(config)#int ___(16)___
RouterB(config-if)#crypto map abc001    //在外部接口上应用加密图
......
```

**【问题 4】（4 分）**

根据题目要求，企业分支机构与总部之间采用 IPSec VPN 技术互连，IPSec（IP Security）是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议应用在___(17)___层，用于保证和认证用户 IP 数据包。

IPSec VPN 可使用的模式有两种，其中___(18)___模式的安全性较强，___(19)___模式的安全性较弱。IPSec 主要由 AH、ESP 和 IKE 组成，在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由___(20)___进行定义。

**试题四分析**

本题考查企业网 IPSec VPN 相关的配置知识。

**【问题 1】**

本问题考查路由器的基本配置命令，主要完成对路由器的基础配置，如地址、加密等。

```
RouterA >enable
```

```
RouterA#configure terminal
RouterA(config)#interface  f0/0
//进入 F0/0 的接口配置子模式
RouterA(config-if)#ip addr 192.168.1.1  255.255.255.0
//为 F0/0 接口配置 IP 地址
RouterA(config-if)#no shut
//开启 F0/0 接口，默认所有路由器的接口都为 down 状态
RouterA(config-if)#inter loopback 0
//进入 loopback 0 的接口配置子模式
RouterA(config-if)#ip addr 192.168.1.20 255.255.255.255
// 为 loopback 0 接口配置 IP 地址
……
RouterA(config)# line vty 0 4
// 进入虚拟接口 0-4 的配置子模式
RouterA(config-line)#password abc001
// 配置 vty 口令为"abc001"
RouterA(config)#enable password abc001
// 配置全局配置模式的明文密码为"abc001"
RouterA(config)# enable secret abc001
// 配置全局配置模式的密文密码为"abc001"
```

**【问题 2】**

本问题考查路由器配置 NAT 转换的相关命令操作。

```
RouterA(config)# access-list 101 deny ip 192.168.1.0 0.0.0.255 172.16.1.0
0.0.0.255
RouterA(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 any
//定义需要被 NAT 的数据流（即除去通过 VPN 要传输的数据流）
RouterA(config)#ip nat inside source list 101 interface s0 overload
//定义 NAT 转换关系
RouterA(config)#int  f0/0
RouterA(config-if)#ip nat inside
RouterA(config)#int s0
RouterA(config-if)#ip nat outside
//在路由器上定义 NAT 的内部和外部接口
…
```

**【问题 3】**

本问题考查配置 IPSec VPN 的具体过程。

```
RouterB(config)#  access-list  102  permit  ip  172.16.1.0   0.0.0.255
192.168.1.0 0.0.0.255
```

```
//定义感兴趣的数据流，即需要通过 VPN 加密传输的数据流
RouterB(config)#crypto isakmp enable
//启用 ISAKMP(IKE) 策略
RouterB(config)#crypto isakmp policy 10
RouterB(config-isakmp)#authentication pre-share
//认证方法使用预共享密钥
RouterB(config-isakmp)#encryption des
//加密方法使用 des
RouterB(config-isakmp)#hash md5
//散列算法使用 md5
RouterB(config-isakmp)#group 2
//DH 模长度为 1024
RouterB(config)#crypto isakmp identity address
RouterB(config)#crypto isakmp key abc001 address 202.102.100.1
//将 ISAKMP 预共享密钥和对等体关联，指定共享密钥和对端设备地址
RouterB(config)#crypto ipsec transform-set ccie esp-des esp-md5-hmac
RouterB(cfg-crypto-trans)#model tunnel
//设置 IPsec 转换集
RouterB(config)#crypto map abc001 10 ipsec-isakmp
......
RouterB(config)#int  s0
RouterB(config-if)#crypto map abc001
//在外部接口上应用加密图
......
```

**【问题 4】**

本问题考查 IPSec VPN 的基础知识。

IPSec（IP Security）是 IETF 为保证在 Internet 上传送数据的安全保密性而制定的框架协议，该协议应用在网络层，用于保证和认证用户 IP 数据包。IPSec 本身是开放的框架式协议，包含的各种算法之间是相互独立的，而且可以确保信息的机密性、数据的完整性、用户的验证和防重发保护，所以在架设 VPN 时通常会使用 IPSec 协议来提供数据安全。

IPSec VPN 可使用的模式有两种，隧道模式和传输模式。使用隧道模式，IPSec 对整个 IP 数据包进行封装和加密，隐蔽了源和目的 IP 地址，从外部看不到数据包的路由过程，比较安全。而传输模式，IPSec 只对 IP 有效数据载荷进行封装和加密，IP 源和目的 IP 地址不加密传送，安全程度较低。

IPSec 主要由 AH、ESP 和 IKE 组成，在使用 IKE 协议时，需要定义 IKE 协商策略，该策略由 SA（安全关联）进行定义。配置 SA 是配置其他 IPSec 的前提，它定义了通信双方保护数据流的策略。

## 参考答案

**【问题 1】**

（1）接口配置

（2）192.168.1.1　255.255.255.0

（3）开启

（4）loopback 0

（5）192.168.1.20　255.255.255.255

（6）line vty 0 4

（7）secret

**【问题 2】**

（8）deny

（9）permit

（10）s0 或者 serial 0

（11）f0/0 或者 fastethernet 0/0

（12）s0 或者 serial 0

**【问题 3】**

（13）172.16.1.0　0.0.0.255　192.168.1.0　0.0.0.255

（14）enable

（15）202.102.100.1

（16）s0 或者 serial 0

**【问题 4】**

（17）网络层

（18）隧道

（19）传输

（20）SA 或者安全关联

# 第 23 章　2014 下半年网络工程师上午试题分析与解答

**试题（1）**

属于 CPU 中算术逻辑单元的部件是＿（1）＿。

（1）A．程序计数器　B．加法器　C．指令寄存器　D．指令译码器

**试题（1）分析**

本题考查计算机系统基础知识。

程序计数器、指令寄存器和指令译码器都是 CPU 中控制单元的部件，加法器是算术逻辑运算单元的部件。

**参考答案**

（1）B

**试题（2）**

内存按字节编址从 A5000H 到 DCFFFH 的区域其存储容量为＿（2）＿。

（2）A．123kb　B．180kb　C．223kb　D．222kb

**试题（2）分析**

本题考查计算机系统基础知识。

从地址 A5000H 到 DCFFFH 的存储单元数目为 37FFFH（即 224*1024）个，由于是字节编址，从而得到存储容量为 224kb。

**参考答案**

（2）D

**试题（3）**

计算机采用分级存储体系的主要目的是为了解决＿（3）＿的问题。

（3）A．主存容量不足　B．存储器读写可靠性

C．外设访问效率　D．存储容量、成本和速度之间的矛盾

**试题（3）分析**

本题考查计算机系统基础知识。

计算机系统中，高速缓存一般用 SRAM，内存一般用 DRAM，外存一般采用磁存储器。SRAM 的集成度低、速度快、成本高，DRAM 的集成度高，但是需要动态刷新。磁存储器速度慢、容量大，价格便宜。因此，组成分级存储体系来解决存储容量、成本和速度之间的矛盾。

**参考答案**

（3）D

**试题（4）**

Flynn 分类法基于信息流特征将计算机分成4类，其中＿（4）＿只有理论意义而无实例。

（4）A．SISD　　B．MISD　　C．SIMD　　D．MIMD

**试题（4）分析**

本题考查计算机系统基础知识。

Flynn 于1972年提出计算平台分类法主要根据指令流和数据流来分类，分为四类：

① 单指令流单数据流机器（SISD）。

SISD 机器是一种传统的串行计算机，它的硬件不支持任何形式的并行计算，所有的指令都是串行执行。并且在某个时钟周期内，CPU 只能处理一个数据流。因此这种机器被称作单指令流单数据流机器。早期的计算机都是 SISD 机器。

② 单指令流多数据流机器（SIMD）。

SIMD 是采用一个指令流处理多个数据流。这类机器在数字信号处理、图像处理，以及多媒体信息处理等领域非常有效。

Intel 处理器实现的 MMXTM、SSE（Streaming SIMD Extensions）、SSE2 及 SSE3 扩展指令集，都能在单个时钟周期内处理多个数据单元。也就是说人们现在用的单核计算机基本上都属于 SIMD 机器。

③ 多指令流单数据流机器（MISD）。

MISD 是采用多个指令流来处理单个数据流。在实际情况中，采用多指令流处理多数据流才是更有效的方法，因此 MISD 只是作为理论模型出现，没有投入实际应用。

④ 多指令流多数据流机器（MIMD）。

MIMD 机器可以同时执行多个指令流，这些指令流分别对不同数据流进行操作。最新的多核计算平台就属于 MIMD 的范畴，例如 Intel 和 AMD 的双核处理器。

**参考答案**

（4）B

**试题（5）**

以下关于结构化开发方法的叙述中，不正确的是＿（5）＿。

（5）A．总的指导思想是自顶向下，逐层分解

B．基本原则是功能的分解与抽象

C．与面向对象开发方法相比，更适合于大规模、特别复杂的项目

D．特别适合于数据处理领域的项目

**试题（5）分析**

本题考查结构化开发方法的基础知识。

结构化开发方法由结构化分析、结构化设计和结构化程序设计构成，是一种面向数据流的开发方法。结构化方法总的指导思想是自顶向下、逐层分解，基本原则是功能的分解与抽象。它是软件工程中最早出现的开发方法，特别适合于数据处理领域的问题，但是不适合解决大规模的、特别复杂的项目，而且难以适应需求的变化。

**参考答案**

（5）C

**试题（6）**

模块 A、B 和 C 都包含相同的 5 个语句，这些语句之间没有联系。为了避免重复，把这 5 个语句抽取出来组成一个模块 D，则模块 D 的内聚类型为＿（6）＿内聚。

（6）A．功能　　B．通信　　C．逻辑　　D．巧合

**试题（6）分析**

本题考查软件设计的相关知识。

模块独立性是创建良好设计的一个重要原则，一般采用模块间的耦合和模块的内聚两个准则来进行度量。内聚是指模块内部各元素之间联系的紧密程度，内聚度越高，则模块的独立性越好。内聚性一般有以下几种：

① 巧合内聚，指一个模块内的各个处理元素之间没有任何联系。

② 逻辑内聚，指模块内执行几个逻辑上相似的功能，通过参数确定该模块完成哪一个功能。

③ 时间内聚，把需要同时执行的动作组合在一起形成的模块。

④ 通信内聚，指模块内所有处理元素都在同一个数据结构上操作，或者指各处理使用相同的输入数据或者产生相同的输出数据。

⑤ 顺序内聚，指一个模块中各个处理元素都密切相关于同一功能且必须顺序执行，前一个功能元素的输出就是下一个功能元素的输入。

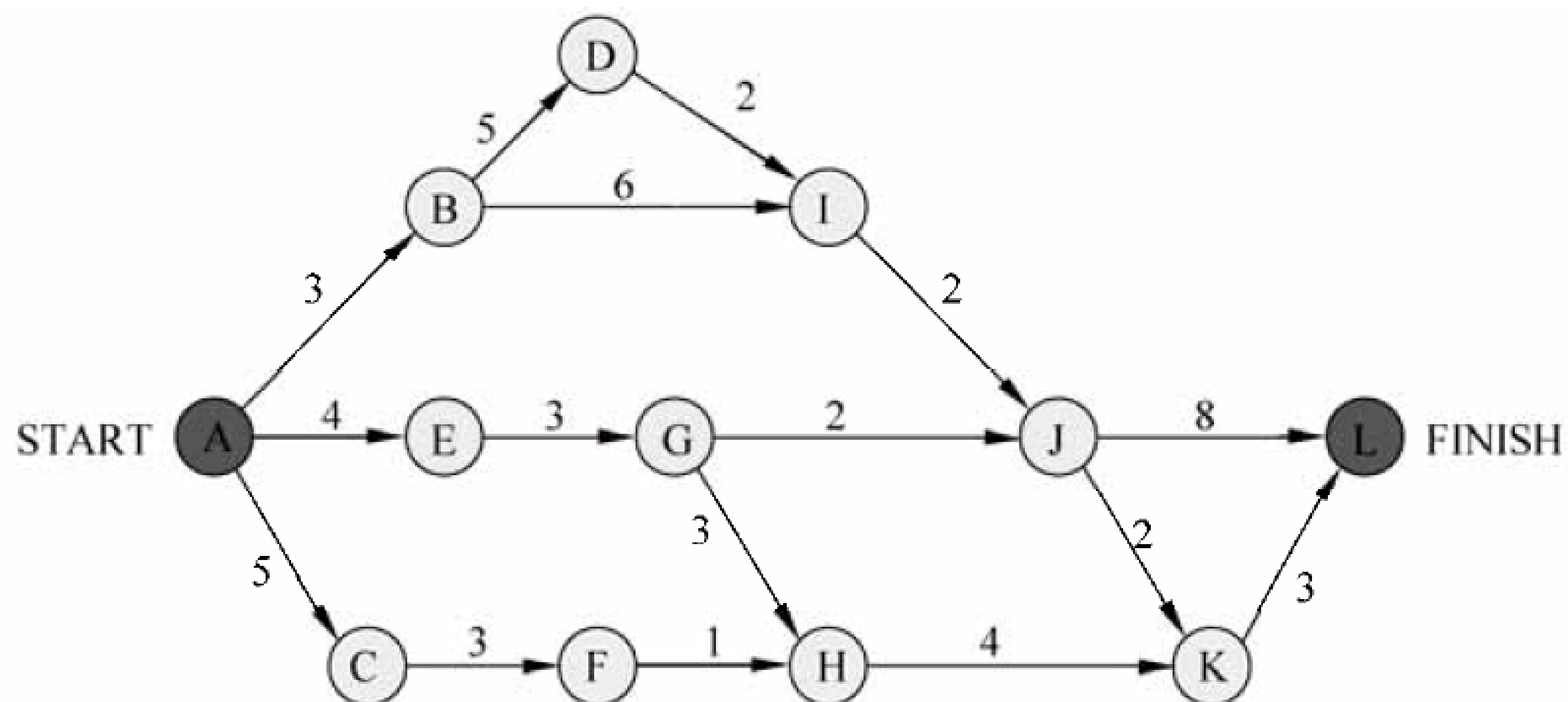
⑥ 功能内聚，是最强的内聚，指模块内所有元素共同完成一个功能，缺一不可。

**参考答案**

（6）D

**试题（7）、（8）**

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边的权重表示活动的持续时间，则里程碑＿（7）＿在关键路径上。活动 GH 的松弛时间是＿（8）＿。




（7）A．B　　B．E　　C．C　　D．K

（8）A．0　　B．1　　C．2　　D．3

**试题（7）、（8）分析**

本题考查活动图的基础知识。

根据关键路径法，计算出关键路径为 A→B→D→I→J→L，其长度为 20。因此里程碑 B 在关键路径上，而里程碑 E、C 和 K 不在关键路径上。包含活动 GH 的最长路径是 A→E→G→H→K→L，长度为 17，因此该活动的松弛时间为 20−17=3。

**参考答案**

（7）A　（8）D

**试题（9）**

将高级语言源程序翻译成机器语言程序的过程中，常引入中间代码。以下关于中间代码的叙述中，不正确的是＿（9）＿。

（9）A．中间代码不依赖于具体的机器

B．使用中间代码可提高编译程序的可移植性

C．中间代码可以用树或图表示

D．中间代码可以用栈和队列表示

**试题（9）分析**

本题考查程序语言基础知识。

从原理上讲，对源程序进行语义分析之后就可以直接生成目标代码，但由于源程序与目标代码的逻辑结构往往差别很大，特别是考虑到具体机器指令系统的特点，要使翻译一次到位很困难，而且用语法制导方式机械生成的目标代码往往是烦琐和低效的，因此有必要设计一种中间代码，将源程序首先翻译成中间代码表示形式，以利于进行与机器无关的优化处理。由于中间代码实际上也起着编译器前端和后端分水岭的作用，所以使用中间代码也有助于提高编译程序的可移植性。常用的中间代码有后缀式、三元式、四元式和树（图）等形式。

**参考答案**

（9）D

**试题（10）**

甲公司接受乙公司委托开发了一项应用软件，双方没有订立任何书面合同。在此情形下，＿（10）＿享有该软件的著作权。

（10）A．甲公司　　B．甲、乙公司共同
　　　C．乙公司　　D．甲、乙公司均不

**试题（10）分析**

委托开发软件著作权关系的建立，通常由委托方与受委托方订立合同而成立。委托开发软件关系中，委托方的责任主要是提供资金、设备等物质条件，并不直接参与开发软件的创作开发活动。受托方的主要责任是根据委托合同规定的目标开发出符合条件的软件。关于委托开发软件著作权的归属，《计算机软件保护条例》第十二条规定："受他人委托开发的软件，其著作权的归属由委托者与受委托者签定书面协议约定，如无书面协议或者在协议中未作明确约定，其著作权属于受委托者。"根据该条的规定，确定委托开发的软件著作权的归属应当掌握两条标准：

① 委托开发软件系根据委托方的要求，由委托方与受托方以合同确定的权利和义务的关系而进行开发的软件，因此软件著作权归属应当作为合同的重要条款予以明确约定。对于当事人已经在合同中约定软件著作权归属关系的，如事后发生纠纷，软件著作权的归属仍应当根据委托开发软件的合同来确定。

② 对于在委托开发软件活动中，委托者与受委托者没有签定书面协议，或者在协议中未对软件著作权归属作出明确的约定，其软件著作权属于受委托者，即属于实际完成软件的开发者。

**参考答案**

（10）A

**试题（11）、（12）**

思科路由器的内存体系由多种存储设备组成，其中用来存放 IOS 引导程序的是＿（11）＿，运行时活动配置文件存放在＿（12）＿中。

（11）A．FLASH　　B．ROM
　　　C．NVRAM　　D．DRAM

（12）A．FLASH　　B．ROM
　　　C．NVRAM　　D．DRAM

**试题（11）、（12）分析**

路由器采用了不同类型的内存，各种内存以不同方式支持路由器运行。闪存（Flash）是可读可写的存储器，在系统重新启动或关机之后仍能保存数据。Flash 中存放着当前使用的 IOS。如果 Flash 容量足够大，甚至可以存放多个操作系统，这在 IOS 升级时十分

有用。当不知道新版 IOS 是否稳定时，可在升级后仍保留旧版 IOS，当出现问题时可退回到旧版操作系统，从而避免长时间的网路故障。

只读存储器 ROM 在路由器中与在计算机中的功能相似，用于系统初始化等。ROM 中包含：系统加电自检代码 POST，用于检测路由器中各种硬件是否完好；系统引导代码（BootStrap）用于启动路由器并载入 IOS 操作系统；备份的 IOS 操作系统，以便在原有 IOS 操作系统被删除或破坏时使用，通常这个 IOS 比现运行 IOS 的版本低一些，但却足以使路由器启动和工作。

非易失性 RAM（Nonvolatile RAM）是可读可写的存储器，在系统重启或关机之后仍能保存数据。NVRAM 速度较快，成本也较高。NVRAM 仅用于保存启动配置文件（Startup-Config），故其容量较小，通常在路由器中只配置 32kb～128kb 的 NVRAM。

动态随机存储器 DRAM 也是可读可写的存储器，但是存储的内容在系统重启或关机后会被清除。RAM 的存取速度比上面 3 种存储器都快。路由器运行时，RAM 中存储路由表、ARP 缓冲区、运行日志和排队等待发送的分组，还包括运行配置文件（Running-config）、正在执行的代码、IOS 操作系统程序和一些临时数据等信息。

**参考答案**

（11）B （12）D

**试题（13）**

下面的广域网络中属于电路交换网络的是<u>（13）</u>。

（13）A. ADSL B. X.25 C. FRN D. ATM

**试题（13）分析**

ADSL 用于连接公共交换电话网 PSTN。PSTN 属于电路交换网，所以 ADSL 是电路交换网的一部分。X.25、FRN 和 ATM 都是分组交换网。

**参考答案**

（13）A

**试题（14）**

PCM 编码是把模拟信号数字化的过程，通常模拟话音信道的带宽是 4000Hz，则在数字化时采样频率至少为<u>（14）</u>次/秒。

（14）A. 2000 B. 4000 C. 8000 D. 16000

**试题（14）分析**

将模拟信号（例如声音、图像等）变换成数字信号，经传输到达接收端再还原为模拟信号，这种技术叫作脉冲编码调制（Pulse Code Modulation，PCM）技术。PCM 主要经过 3 个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续、幅度连续的模拟信号变换为时间离散、幅度连续的采样信号；量化过程将采样信号变为时间离散、幅度离散的数字信号；编码过程将量化后的离散信号编码为二进制码组。采样频率决定了可恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样

频率必须大于模拟信号最高频率的二倍，即

$$f=\frac{1}{T}>2f_{\max}$$

其中，$f$ 为采样频率，$T$ 为采样周期，$f_{\max}$ 为信号的最高频率。通常模拟话音信道的带宽（即最高频率）是 4000Hz，所以在数字化时采样频率至少为 8000 次/秒。

**参考答案**

（14）C

**试题（15）**

设信道带宽为 4000Hz，信噪比为 30dB，按照香农定理，信道容量为__（15）__。

（15）A．4kb/s　　B．16kb/s　　C．40kb/s　　D．120kb/s

**试题（15）分析**

尼奎斯特定理指出：若信道带宽为 W，则最大码元速率为

$$B=2W\text{（Baud）}$$

这是由信道的物理特性决定的，是在无噪声的理想情况下的极限值。实际信道会受到各种噪声的干扰，因而达不到按尼奎斯特定理计算出的数据传送速率。香农（Shannon）的研究表明，有噪声信道的极限数据速率可由下面的公式计算：

$$C=W\log_2(1+\frac{S}{N})$$

这个公式叫作香农定理。其中，$W$ 为信道带宽，$S$ 为信号的平均功率，$N$ 为噪声的平均功率，$S/N$ 叫作信噪比。由于在实际使用中 $S$ 与 $N$ 的比值太大，故常取其分贝数(dB)。分贝与信噪比的关系为 $SNR_{DB}=10\log_{10}(S/N)$，例如当 $S/N=1000$ 时，信噪比为 30dB。这个公式表明，无论用什么方式调制，只要给定了信噪比，则单位时间内可传输的最大信息量就确定了，所以称为信道容量。本题中信道带宽为 4 000Hz，信噪比为 30dB，则最大数据速率为

$$C=4\,000\log_2(1+1\,000)\cong 4\,000\times 9.97\cong 40\,000\text{ b/s}=40\text{kb/s}$$

这是极限值，只有理论上的意义。

**参考答案**

（15）C

**试题（16）**

所谓正交幅度调制是把两个__（16）__的模拟信号合成为一个载波信号。

（16）A．幅度相同相位相差 90°　　B．幅度相同相位相差 180°

C．频率相同相位相差 90°　　D．频率相同相位相差 180°

**试题（16）分析**

正交幅度调制（Quadrature Amplitude Modulation，QAM）是把两个幅度相同但相位相差 90° 的模拟信号合成为一个载波信号，经过信道编码后把数据组合映射到星座图上，

如下图所示。

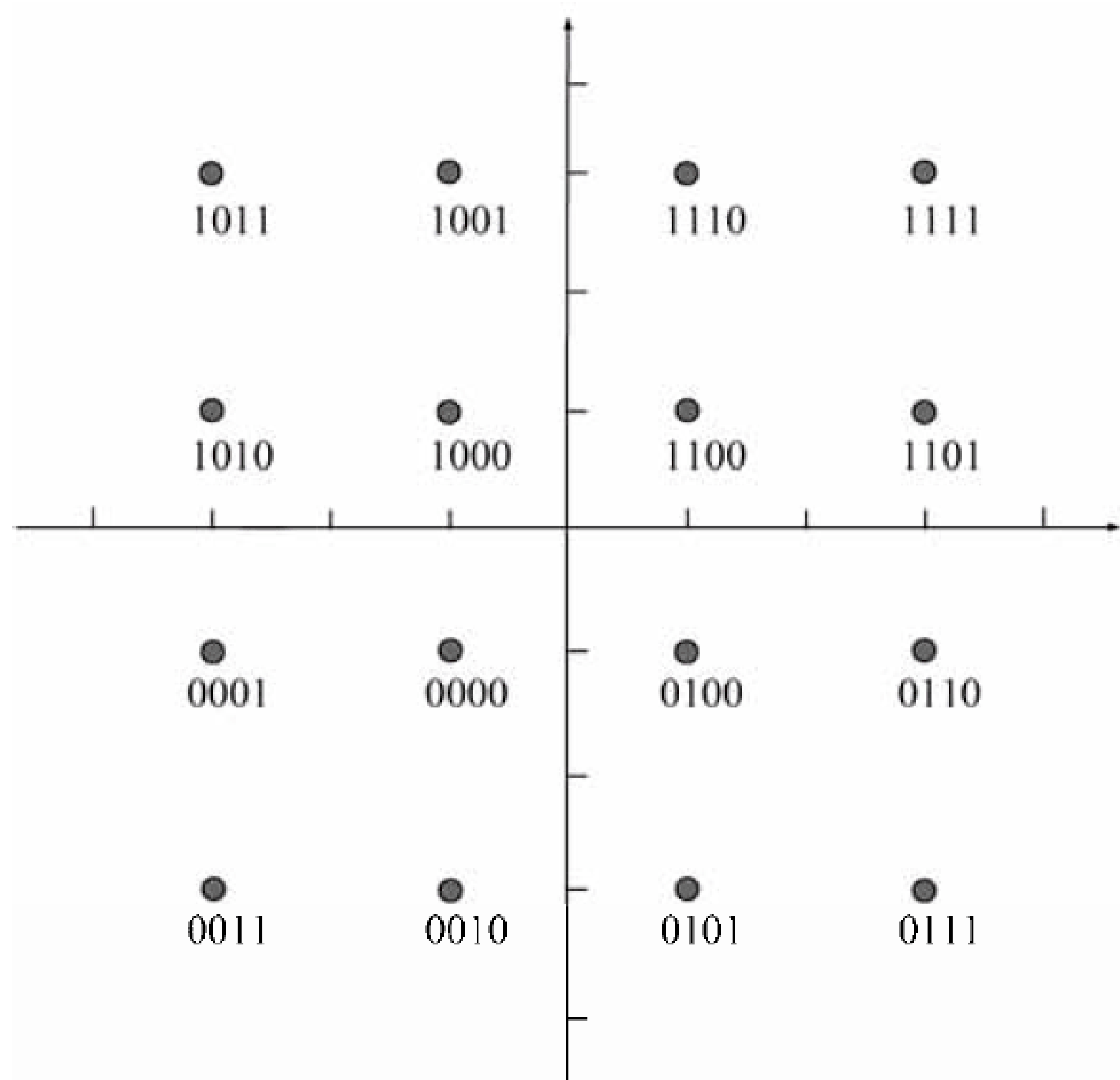



图 QAM 调制

QAM 调制实际上是幅度调制和相位调制的组合，同时利用了载波的幅度和相位来传递数据信息。与单纯的 PSK 调制相比，在最小距离相同的条件下，QAM 星座图中可以容纳更多的载波码点，可以实现更高的频带利用率。

**参考答案**

（16）A

**试题（17）、（18）**

电信运营商提供的 ISDN 服务有两种不同的接口，其中供小型企业和家庭使用的基本速率接口（BRI）可提供的最大数据速率为__（17）__，供大型企业使用的主速率接口（PRI）可提供的最大数据速率为__（18）__。

（17）A．128kb/s　　B．144kb/s　　C．1024kb/s　　D．2048kb/s

（18）A．128kb/s　　B．144kb/s　　C．1024kb/s　　D．2048kb/s

**试题（17）、（18）分析**

ISDN 分为窄带 ISDN（Narrowband ISDN，N-ISDN）和宽带 ISDN（Broadband ISDN，B-ISDN）。N-ISDN 的目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一个网络上统一传输。ISDN 系统提供两种用户接口：即基本速率 2B+D 和基群速率 30B+D。所谓 B 信道是 64kb/s 的话音或数据信道，而 D 信道是 16kb/s 或 64kb/s 的信令信道。对于家庭用户，通信公司在用户住所安装一个第一类网络终接设备 NT1。用户可以在连接 NT1 的总线上最多挂接 8 台设备，共享 2B+D 的 144kb/s 信道。大型商业用户

则要通过第二类网络终接设备 NT2 连接 ISDN，这种接入方式可以提供 30B+D（2.048Mb/s）的接口速率。

**参考答案**

（17）B　（18）D

**试题（19）**

PPP 是网络交换设备连接广域网的一种封装协议，下面关于 PPP 的描述中错误的是<u>（19）</u>。

（19）A．能够控制数据链路的建立

B．能够分配和管理广域网的 IP 地址

C．只能采用 IP 作为网络层协议

D．能够有效地进行错误检测

**试题（19）分析**

点对点协议应用在许多场合，例如家庭用户拨号上网，或者局域网通过租用公网专线远程联网等。常用的点对点协议是 PPP 协议（Point-to-Point Protocol）。事实上，PPP 是一组协议，其中包括：

- 链路控制协议 LCP（Link Control Protocol），用于建立、释放和测试数据链路，以及协商数据链路参数；
- 网络控制协议 NCP（Network Control Protocol），用于协商网络层参数，例如动态分配 IP 地址等；
- 身份认证协议，用于通信双方确认对方的链路标识。

PPP 帧的封装格式（如下图所示）类似于 HDLC。

| 1 | 1 | 1 | 1或2 | 可变长 | 2或4 | 1 |
|---|---|---|---|---|---|---|
| 帧标志F 01111110 | 地址A 11111111 | 控制C 00000011 | 协议 | INFO | FCS | 帧标志F 01111110 |

图　PPP 的帧结构

PPP 的地址字段为全 1，表示广播地址。控制字段取值 0x03，表示无编号帧。PPP 的协议字段用于标识信息字段（INFO）中封装的数据报。PPP 可以支持任何网络层协议，例如 IP、IPX、AppleTalk、OSI CLNP、XNS 等。PPP 的负载（INFO）长度默认为 1500 个字节。校验和（FCS）长度是可协商的，可以使用 16 位或 32 位的校验码。

**参考答案**

（19）C

**试题（20）、（21）**

下面关于帧中继的描述中错误的是<u>（20）</u>，思科路由器支持的帧中继本地管理接口类型（Lmi-type）不包括<u>（21）</u>。

（20）A．在第三层建立虚电路

B．提供面向连接的服务

C．是一种高效率的数据链路技术

D．充分利用了光纤通信和数字网络技术的优势

（21）A．Cisco　　B．DCE　　C．ANSI　　D．Q933A

**试题（20）、（21）分析**

帧中继（Frame Relay，FR）网络运行在 OSI 参考模型的物理层和数据链路层。FR 用第二层的帧承载数据业务，因而第三层被省掉了。帧中继提供面向连接的服务，在互相通信的每对设备之间都存在一条定义好的虚电路，并且指定了一个链路识别码 DLCI。帧中继利用了光纤通信和数字网络技术的优势，FR 帧层操作比 HDLC 简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。所以，帧中继比 X.25 具有更高的传输效率。

普通路由器就可以配置成帧中继交换机。在路由器串行接口配置 FR 封装的命令如下表所示，可设置的本地管理接口类型有 3 种{ansi | cisco | q933a}

| 命　　令 | 功　　能 |
| --- | --- |
| encapsulation frame-relay[ietf] | 设置 Frame Relay 封装 |
| frame-relay lmi-type {ansi | cisco | q933a} | 设置 Frame Relay LMI 类型 |
| interface interface-type interface-number subinterface-number [multipoint|point-to-point] | 设置子接口 |
| frame-relay map protocol protocol-address dlci [broadcast] | 映射协议地址与 DLCI |
| frame-relay interface-dlci dlci [broadcast] | 设置 FR DLCI 编号 |

**参考答案**

（20）A　（21）B

**试题（22）、（23）**

边界网关协议 BGP4 被称为路径矢量协议，它传送的路由信息是由一个地址前缀后跟（22）组成，这种协议的优点是（23）。

（22）A．一串 IP 地址　　B．一串自治系统编号

C．一串路由器编号　　D．一串子网地址

（23）A．防止域间路由循环　　B．可以及时更新路由

C．便于发现最短通路　　D．考虑了多种路由度量因素

**试题（22）、（23）分析**

边界网管协议 BGP 是应用于自治系统（AS）之间的外部网关协议。BGP4 基本上是一个距离矢量路由协议，但是与 RIP 协议采用的算法稍有区别。BGP 不但为每个目标计算最小通信费用，而且跟踪通向目标的路径；它不但把目标的通信费用发送给每一个邻居，而且也公告通向目标的最短路径（由 AS 编号的列表组成）。所以 BGP4 被称为路径

矢量协议。

BGP 算法没有距离矢量路由协议的不稳定性，可以避免路由循环。当 BGP 路由器收到一条路由信息时，首先检查它所在的自治系统是否在路径列表中。如果在列表中，则该路由信息被忽略，从而避免了出现路由循环。

BGP4 支持无类别的域间路由（CIDR），BGP 邻居之间通过 TCP 连接端口 179 交换路由信息。这意味着 BGP4 可以利用 TCP 连接的差错和流量控制功能。当检测到路由表改变时，BGP 只把改变了路由通过 TCP 连接发送给它的邻居。

**参考答案**

（22）B　（23）A

**试题（24）**

与 RIPv2 相比，IGRP 协议增加了一些新的特性，下面的描述中错误的是__（24）__。

（24）A．路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数

B．增加触发更新来加快路由收敛，不必等待更新周期结束再发送更新报文

C．不但支持相等费用通路负载均衡，而且支持不等费用通路的负载均衡

D．最大跳步数由 15 跳扩大到 255 跳，可以支持更大的网络

**试题（24）分析**

内部网关路由协议（Interior Gateway Routing Protocol，IGRP）是 Cisco 公司 1980 年代设计的一种动态距离矢量路由协议。它组合了网络配置的各种因素，包括带宽、延迟、可靠性和负载等作为路由度量。它支持相等费用通路负载均衡和不等费用通路负载均衡。IGRP 的最大跳步数由 15 跳扩大到 255 跳，可以支持比 RIPv2 更大的网络。

默认情况下，IGRP 每 90s 发送一次路由更新广播，在 3 个更新周期内（即 270s）没有从某个路由器接收到更新报文，则宣布该路由不可访问。在 7 个更新周期即 630s 后，IOS 从路由表中清除该路由表项。

用触发更新来加快路由收敛，这是 RIPv2 和 IGRP 都有的功能。

**参考答案**

（24）B

**试题（25）**

为了解决 RIP 协议形成路由环路的问题可以采用多种方法，下面列出的方法中效果最好的是__（25）__。

（25）A．不要把从一个邻居学习到的路由发送给那个邻居

B．经常检查邻居路由器的状态，以便及时发现断开的链路

C．把从邻居学习到的路由设置为无限大，然后再发送给那个邻居

D．缩短路由更新周期，以便出现链路失效时尽快达到路由无限大

**试题（25）分析**

距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路

由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。

解决路由环路问题可以采用水平分割法（Split Horizon）。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。如果每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。

简单的水平分割方案是："不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是："把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居"。采用反向毒化的方案更安全一些，可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，触发更新技术也能加快路由收敛，如果触发更新足够及时，则也可以防止环路的形成。

**参考答案**

（25）C

**试题（26）、（27）**

城域以太网在各个用户以太网之间建立多点第二层连接，IEEE 802.1ah 定义的运营商主干网桥协议提供的基本技术是在用户以太帧中再封装一层__（26）__，这种技术被称为__（27）__技术。

（26）A．运营商的 MAC 帧头　　B．运营商的 VLAN 标记
　　　C．用户 VLAN 标记　　D．用户帧类型标记

（27）A．Q-in-Q　　B．IP-in-IP
　　　C．NAT-in-NAT　　D．MAC-in-MAC

**试题（26）、（27）分析**

城域以太网论坛（MEF）定义的 IEEE 802.1ah 标准提出了运营商主干网桥（Provider Backbone Bridge，PBB）协议。所谓主干网桥就是运营商网络边界的网桥，通过 PBB 对用户以太帧再封装一层运营商的 MAC 帧头，添加主干网目标地址和源地址（B-DA，B-SA）、主干网 VLAN 标识（B-VID）以及服务标识（I-SID）等字段。由于用户以太帧被封装在主干网以太帧中，所以这种技术被称为 MAC-in-MAC 技术。

按照 802.1ah 协议，主干网与用户网具有不同的地址空间。主干网的核心交换机只处理通常的以太网帧头，仅主干网边界交换机才具有 PBB 功能。这样，用户网和主干网被 PBB 隔离，使得扁平式的以太网变成了层次化结构，简化了网络管理，保证了网络安全。802.1ah 协议规定的服务标识（I-SID）字段为 24 位，可以区分 1600 万种不同的服务，使得网络的扩展性得以提升。由于采用了二层技术，没有复杂的信令机制，因此设备成本和维护成本较低，被认为是城域以太网的最终解决方案。IEEE 802.1ah 与其他局域网协议的关系参见下图。

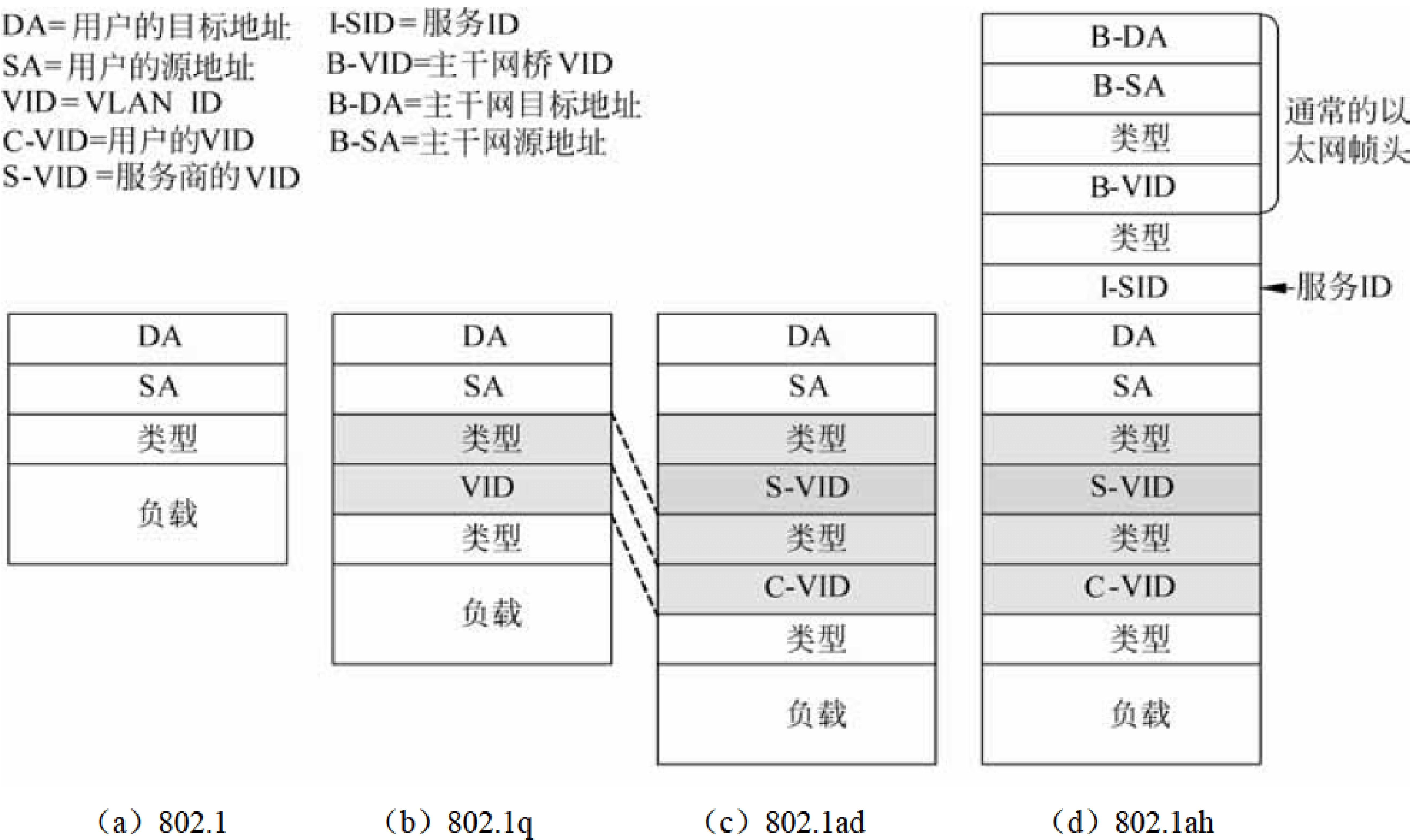


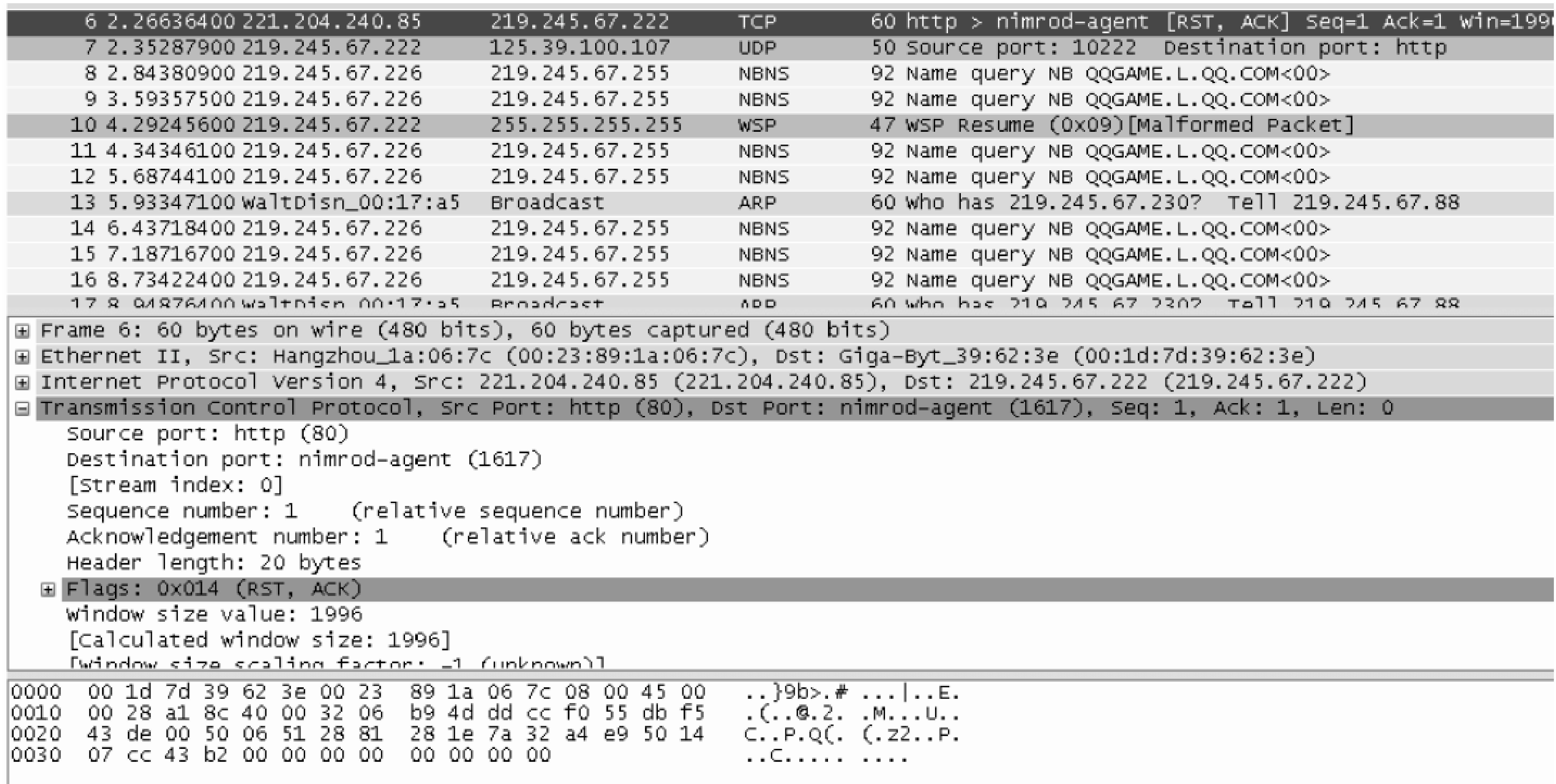

图　城域以太网的帧格式

**参考答案**

（26）A　（27）D

**试题（28）、（29）**

采用抓包工具截获的结果如下图所示，图中第 1 行记录显示的是__（28）__，该报文由__（29）__发出。



（28）A．TCP 错误连接响应报文　　B．TCP 连接建立请求报文
　　C．TCP 连接建立响应报文　　D．Urgent 紧急报文

（29）A．Web 客户端　　B．Web 服务器
　　C．DNS 服务器　　D．DNS 客户端

**试题（28）、（29）分析**

本题考查网络管理工具的应用及 TCP 协议原理。

从图中的标志字段为 RST 和 ACK 可以看出，该报文为 TCP 连接出现错误，并进行捎带应答。该记录的源端口号为 80，表明发出报文的是 Web 服务器端。

**参考答案**

（28）A　（29）B

**试题（30）**

在 Windows 命令行窗口中键入 tracert 命令得到下图所示窗口，则该 PC 的 IP 地址可能为__（30）__。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\User>tracert news.sina.com.cn

Tracing route to ara.sina.com.cn [58.63.236.45]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  219.245.67.254
  2     1 ms     1 ms     1 ms  172.16.11.2
  3    <1 ms    <1 ms    <1 ms  172.16.255.254
  4     1 ms     1 ms     1 ms  61.150.43.65
  5    15 ms     1 ms     7 ms  10.224.11.5
  6     *        4 ms     2 ms  117.36.240.33
  7    34 ms    36 ms    35 ms  202.97.78.113
  8    35 ms    35 ms    36 ms  113.108.208.2
  9    32 ms    32 ms    32 ms  113.108.209.74
 10    32 ms    32 ms    33 ms  58.63.232.217
 11    32 ms    33 ms    32 ms  58.63.236.45

Trace complete.

C:\Documents and Settings\User>_
```

（30）A．172.16.11.13　　B．113.108.208.1
　　C．219.245.67.5　　D．58.63.236.45

**试题（30）分析**

本题考查网络管理命令及其含义。

tracert 命令查看的是从本机出发到目的主机时经过的所有路由器及三个延迟时间。第 1 条记录是本机的网关，主机应与网关在一个网段。

**参考答案**

（30）C

**试题（31）**

管理员为某台 Linux 系统中的/etc/hosts 文件添加了如下记录，下列说法中正确的是__（31）__。

127.0.0.1 localhost.localdomain localhost

192.168.1.100 linumu100.com web80

192.168.1.120 emailserver

（31）A．linumu100.com 是主机 192.168.1.100 的主机名

B．web80 是主机 192.168.1.100 的主机名

C．emailserver 是主机 192.168.1.120 的别名

D．192.168.1.120 行记录的格式是错误的

**试题（31）分析**

本题考查 Linux 文件系统的基础知识。

Linux 文件系统中的/etc/hosts 文件包含了 IP 地址和主机名之间的映射关系，包括系统的别名（可以没有），记录的顺序为：

IP 地址　主机名　别名

**参考答案**

（31）A

**试题（32）**

下列关于 Linux 文件组织方式的说法中，__（32）__是错误的。

（32）A．Linux 文件系统使用索引节点来记录文件信息

B．文件索引节点号由管理员手工分配

C．每个文件与唯一的索引节点号对应

D．一个索引节点号可对应多个文件

**试题（32）分析**

本题考查 Linux 文件系统的基础知识。

Linux 文件系统使用索引节点来记录文件信息，作用与 Windows 的文件分配表类似。索引节点是一个数据结构，它包含了一个文件的文件名、位置、大小、建立或修改时间、访问权限、所属关系等文件控制信息。一个文件系统维护了一个索引节点的数组，每个文件或目录都与索引节点数组中的唯一一个元素对应。系统为每个索引节点分配了一个号码，也就是该节点在数组中的索引号，称为索引节点号。

Linux 文件系统将文件索引节点号和文件名同时保存在目录中。所以，目录只是将文件的名称和它的索引节点号结合在一起的一张表，目录中每一对文件名称和索引节点号称为一个连接。对于每个文件都有一个唯一的索引节点号与之对应，而对于一个索引节点号，却可以有多个文件名与之对应。因此，在磁盘上的同一个文件可以通过不同的路径去访问它。

**参考答案**

（32）B

**试题（33）**

netstat-r 命令的功能是（33）。

（33）A．显示路由记录　　B．查看连通性
　　C．追踪 DNS 服务器　　D．捕获网络配置信息

**试题（33）分析**

本题考查网络管理命令及其含义。

netstat-r 命令的功能是显示路由记录。

**参考答案**

（33）A

**试题（34）**

搭建试验平台、进行网络仿真是网络生命周期中（34）阶段的任务。

（34）A．需求规范　　B．逻辑网络设计
　　C．物理网络设计　　D．实施

**试题（34）分析**

本题考查网络生命周期。

逻辑网络设计的任务包括搭建试验平台、进行网络仿真。

**参考答案**

（34）B

**试题（35）**

在 Windows 系统中可通过停止（35）服务来阻止对域名解析 Cache 的访问。

（35）A．DNS Server　　B．Remote Procedure Call（RPC）
　　C．Nslookup　　D．DNS Client

**试题（35）分析**

本题考查网络操作系统及服务器配置。

DNS Client 是一个访问本地域名解析 Cache 的组件。

**参考答案**

（35）D

**试题（36）、（37）**

某公司域名为 pq.com，其 POP 服务器的域名为 pop.pq.com，SMTP 服务器的域名为 smtp.pq.com，配置 Foxmail 邮件客户端时，在发送邮件服务器栏应该填写（36），在接收邮件服务器栏应该填写（37）。

（36）A．pop.pq.com　B．smtp.pq.com　C．pq.com　D．pop3.pq.com

（37）A．pop.pq.com　B．smtp.pq.com　C．pq.com　D．pop3.pq.com

**试题（36）、（37）分析**

本题考查邮件服务器的基础知识。

SMTP 协议和 POP 协议是邮件服务器的两个重要协议。SMTP 协议用于邮件的发送，POP 协议用于邮件的接收。Foxmail 是一种常用的桌面邮件客户端，使用该软件时，需设置相应的发送邮件服务器和接收邮件服务器地址，根据题目所给出的发送邮件服务器和接收邮件服务器地址，试题（36）空白处应填写 smtp.pq.com，试题（37）空白处应填写 pop.pq.com。

**参考答案**

（36）B　（37）A

**试题（38）**

在 Linux 操作系统中，采用＿（38）＿来搭建 DNS 服务器。

（38）A．Samble　　B．Tomcat　　C．Bind　　D．Apache

**试题（38）分析**

本题考查 Linux 系统下应用服务器的基础知识。

Tomcat 是 Apache 软件基金会（Apache Software Foundation）的 Jakarta 项目中的一个核心项目，由 Apache、Sun 和其他一些公司及个人共同开发而成，成为目前比较流行的 Web 应用服务器。目前最新版本是 8.0。

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用。当在一台机器上配置好 Apache 服务器，可利用它响应 HTML（标准通用标记语言下的一个应用）页面的访问请求。Tomcat 部分是 Apache 服务器的扩展，它独立运行，因此当运行 tomcat 时，它实际上是作为一个与 Apache 独立的进程单独运行的。

BIND（Berkeley Internet Name Daemon）是现今互联网上最常使用的 DNS 服务器软件，使用 BIND 作为服务器软件的 DNS 服务器约占所有 DNS 服务器的九成。BIND 现在由互联网系统协会（Internet Systems Consortium）负责开发与维护。

Apache 是一种广为使用的 Web 服务器软件。它可以运行在几乎所有的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的 Web 服务器端软件。

**参考答案**

（38）C

**试题（39）**

DNS 服务器的默认端口号是＿（39）＿端口。

（39）A．50　　B．51　　C．52　　D．53

**试题（39）分析**

本题考查应用服务器的基础知识。

DNS 是一种在网络上为用户提供从域名向 IP 地址映射的服务。它基于 UDP 运行，使用 53 号端口。

**参考答案**

（39）D

**试题（40）**

使用＿（40）＿命令可以向 FTP 服务器上传文件。

（40）A. get　　B. dir　　C. put　　D. push

**试题（40）分析**

本题考查应用服务器的基础知识。

文件传输协议（File Transfer Protocol，FTP）是在 Internet 中两个远程计算机之间传送文件的协议。该协议允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。通过 FTP 可以传送任意类型、任意大小的文件。FTP 的命令及功能如下。

- dir 命令，用来显示 FTP 服务器端有哪些文件可供下载。
- get 命令，用来从服务器端下载一个文件。
- !dir 命令，用来显示客户端当前目录中的文件信息。
- put 命令，用来向 FTP 服务器端上传一个文件。

**参考答案**

（40）C

**试题（41）**

假设有证书发放机构 $I_1$、$I_2$，用户 A 在 $I_1$ 获取证书，用户 B 在 $I_2$ 获取证书，$I_1$ 和 $I_2$ 已安全交换了各自的公钥，如果用 $I_1$《A》表示由 $I_1$ 颁发给 A 的证书，A 可通过＿（41）＿证书链获取 B 的公开密钥。

（41）A. $I_1$《$I_2$》$I_2$《B》　　B. $I_2$《B》$I_1$《$I_2$》

C. $I_1$《B》$I_2$《$I_2$》　　D. $I_2$《$I_1$》$I_2$《B》

**试题（41）分析**

本题考查证书认证的基础知识。

两个认证机构相互交换了各自公钥之后，用户可使用已有的公钥，验证另一个机构的证书，并从中获取另一个机构的公钥，然后使用获取的另一个机构公钥对该机构下的用户证书进行验证，并从中得到用户公钥。可用以下关系式表达：

用 $I_1$、$I_2$ 表示两个证书颁发机构，用 A 和 B 表示分别从 $I_1$ 和 $I_2$ 处获取证书的两个用户。用《A》$I_1$《A》表示由 $I_1$ 颁发给 A 的证书，关系式如下：$I_1$《$I_2$》$I_2$《B》。

**参考答案**

（41）A

**试题（42）～（44）**

PGP（Pretty Good Privacy）是一种电子邮件加密软件包，它提供数据加密和数字签名两种服务，采用＿（42）＿进行身份认证，使用＿（43）＿（128 位密钥）进行数据加密，使用＿（44）＿进行数据完整性验证。

（42）A．RSA 公钥证书　　B．RSA 私钥证书
　　　C．Kerboros 证书　　D．DES 私钥证书

（43）A．IDEA　　B．RSA　　C．DES　　D．Diffie-Hellman

（44）A．HASH　　B．MD5　　C．三重 DES　　D．SHA-1

**试题（42）～（44）分析**

本题考查 PGP 加密工具的基础知识。

PGP（Pretty Good Privacy）是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。由于该软件违反了美国的密码产品出口限制，作者被联邦政府进行了 3 年的犯罪调查。今天 PGP 已经成为使用最广泛的电子邮件加密软件。PGP 能够得到广泛应用的原因是：

① 能够在各种平台（DOS、Windows、Unix、Macintosh 等）上免费使用，并且得到许多制造商的支持；

② 基于比较安全的加密算法（RSA、IDEA、MD5）；

③ 具有广泛的应用领域，既可用于加密文件，也可用于个人安全通信；

④ 该软件包不是由政府或标准化组织开发和控制的，这一点对于具有自由倾向的网民特别具有吸引力。

PGP 提供两种服务：数据加密和数字签名。数据加密机制可以应用于本地存储的文件，也可以应用于网络上传输的电子邮件。数字签名机制用于数据源身份认证和报文完整性验证。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA（128 位密钥）进行数据加密，使用 MD5 进行数据完整性验证。

**参考答案**

（42）A　（43）A　（44）B

**试题（45）**

以下关于 S-HTTP 的描述中，正确的是＿（45）＿。

（45）A．S-HTTP 是一种面向报文的安全通信协议，使用 TCP 443 端口
　　　B．S-HTTP 所使用的语法和报文格式与 HTTP 相同
　　　C．S-HTTP 也可以写为 HTTPS
　　　D．S-HTTP 的安全基础并非 SSL

**试题（45）分析**

本题考查 S-HTTP 协议的基础知识。

S-HTTP 不是采用 SSL 的安全协议。

**参考答案**

（45）D

**试题（46）**

把交换机由特权模式转换到全局配置模式使用的命令是＿（46）＿。

（46）A. interface f0/1　　B. config terminal
　　　C. enable　　D. no shutdown

**试题（46）分析**

本题考查交换机的模式转换命令。

交换机一般具有用户模式、特权模式、全局模式、端口模式。在特权模式下输入 config terminal（可简写 conf t）命令即可，用户在该模式下可修改交换机的全局配置，如修改主机名等。

**参考答案**

（46）B

**试题（47）**

在无线局域网中，AP（无线接入点）工作在 OSI 模型的＿（47）＿。

（47）A. 物理层　　B. 数据链路层　　C. 网络层　　D. 应用层

**试题（47）分析**

本题考查 AP 的工作模型。

AP 是组建小型无线局域网时最常用的设备。AP 相当于一个连接有线网和无线网的桥梁，工作在数据链路层。其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

**参考答案**

（47）B

**试题（48）**

利用扩展 ACL 禁止用户通过 telnet 访问子网 202.112.111.0/24 的命令是＿（48）＿。

（48）A. access-list 10 deny telnet any 202.112.111.0 0.0.0.255 eq 23
　　　B. access-list 110 deny udp any 202.112.111.0 eq telnet
　　　C. access-list 110 deny tcp any 202.112.111.0 0.0.0.255 eq 23
　　　D. access-list 10 deny tcp any 202.112.111.0 255.255.255.0 eq 23

**试题（48）分析**

本题考查 ACL 配置命令的使用。

首先，利用扩展 ACL 可排除 A 和 D 选项；其次 B 选项中使用了 UDP，Telnet 是基于 TCP 协议的，所以 B 选项错误。

**参考答案**

（48）C

**试题（49）**

以下关于 Windows Server 2003 域管理模式的描述中，正确的是＿（49）＿。

（49）A. 域间信任关系只能是单向信任
　　　B. 单域模型中只有一个主域控制器，其他都为备份域控制器
　　　C. 如果域控制器改变目录信息，应把变化的信息复制到其他域控制器
　　　D. 只有一个域控制器可以改变目录信息

**试题（49）分析**

本题考查 Windows Server 2003 域管理模式的知识。

域信任关系是一种建立在域间的关系，它使得一个域中的用户可以由另一个域中的域控制器进行验证。在所有域关系中只有两种域，即信任关系域和被信任关系域。在 Windows Server 2003 之间可以建立如下信任关系：传递信任关系、不传递信任关系、单向信任关系、双向信任关系。一个域中可以有任意多个域控制器，但只有一个拥有 FSMO 角色。每个域控制器都可以改变目录信息，并把变化的信息复制到其他域控制器。

**参考答案**

（49）C

**试题（50）**

SNMPv2 的__（50）__操作为管理站提供了从被管设备中一次取回一批数据的能力。

（50）A．GetNextRequest　　B．InformRequest
　　　C．SetRequest　　D．GetBulkRequest

**试题（50）分析**

本题考查 SNMPv2 的知识。

SNMPv2 增加了一种新的操作类型 GetBulkRequest 操作，能够有效地检索大块的数据，特别是能够有效地检索大块的数据，适合在表中检索多行数据，其为管理站提供了从被管设备中一次取回一批数据的能力。

**参考答案**

（50）D

**试题（51）、（52）**

DNS 服务器中的资源记录分成不同类型，其中指明区域主服务器和管理员邮件地址的是__（51）__，指明区域邮件服务器地址的是__（52）__。

（51）A．SOA 记录　　B．PTR 记录　　C．MX 记录　　D．NS 记录

（52）A．SOA 记录　　B．PTR 记录　　C．MX 记录　　D．NS 记录

**试题（51）、（52）分析**

DNS 服务器中的资源记录（Resource Record）分成不同类型，常用类型有（参见表 2）：

① SOA（Start Of Authoritative）：开始授权记录是区域文件的第一条记录，指明区域的主服务器，指明区域管理员的邮件地址，并给出区域复制的有关信息。例如序列号、刷新间隔、有效期和生命周期（TTL）等；

② A（Address）：地址记录表示主机名到 IP 地址的映射；

③ PTR（Pointer）：指针记录是 IP 地址到主机名的映射；

④ NS（Name Server）：名字服务器记录给出区域的授权服务器；

⑤ MX（Mail eXchanger）：邮件服务器记录定义了区域的邮件服务器及其优先级；

⑥ CNAME：别名记录为正式主机名定义了一个别名（alias）。

表　资源记录

| 记录类型 | 说　　明 | 示　　例 |
|---|---|---|
| 开始授权（SOA） | 指明区域主服务器（primary nameserver）<br>指明区域管理员的邮件地址，及区域复制信息<br>序列号<br>刷新间隔<br>重试间隔<br>有效期<br>TTL | 区域 microsoft.com<br>的主服务器为 ns1.microsoft.com<br>2003080800　;serial number<br>172800　;refresh=2d<br>900　;retry=15m<br>1209600　;expire=2w<br>3600　;default TTL=1h |
| 地址（A） | 最常用的资源记录<br>把主机名解析为 IP 地址 | compuer1.microsoft.com 被解析为 10.1.1.4 |
| 指针（PTR） | 用于反向查询的资源记录<br>把 IP 地址解析为主机名 | 10.1.1.4 被解析为 compuer1.microsoft.com |
| 名字服务器（NS） | 为一个域指定了授权服务器<br>该域的所有子域也被委派给这个服务器 | 域 microsoft.com 的授权服务器为 ns2.microsoft.com |
| 邮件服务器（MX） | 指明区域的 SMTP 服务器 | 区域 microsoft.com 的邮件服务器为 mail.microsoft.com |
| 别名（CNAME） | 指定主机的别名<br>把主机名解析为另一个主机名 | www.microsoft.com 的别名为 webserver12.microsoft.com |

**参考答案**

（51）A　（52）C

**试题（53）**

以下地址中属于自动专用 IP 地址（APIPA）的是__（53）__。

（53）A．224.0.0.1　　B．127.0.0.1

C．192.168.0.1　　D．169.254.1.15

**试题（53）分析**

选项中的 4 个地址分别是：224.0.0.1 为组播地址；127.0.0.1 为本地环路地址，用于测试本地 TCP/IP 协议栈是否工作正常；192.168.0.1 为 C 类私网地址；169.254.1.15 属于微软定义的自动专用 IP 地址。在采用动态分配地址的网络中，当出现由于 DHCP 服务器故障而不能获得自动分配的 IP 地址时，主机自动获得 169.254.0.0 网络中一个互不冲突的地址。

**参考答案**

（53）D

**试题（54）**

公司得到一个 B 类网络地址块，要划分成若干个包含 1000 台主机的子网，则可以划分成多少个子网？__（54）__

（54）A．100　　B．64　　C．128　　D．500

**试题（54）分析**

一个 B 类地址块包含 16 位主机地址码，1000 台主机需要 10 位主机地址码，剩余的 6 位可以提供 64 个子网号。

**参考答案**

（54）B

**试题（55）**

IP 地址 202.117.17.254/22 是什么地址？（55）

（55）A．网络地址　　B．全局广播地址

C．主机地址　　D．定向广播地址

**试题（55）分析**

IP 地址 202.117.17.254/22 的二进制形式是 **11001010 01110101 000100**01 11111110，其中的黑体部分为网络地址，其他部分为主机地址。由于主机地址部分既不为全 0（表示网络地址），也不为全 1（表示广播地址），所以它是主机地址。

**参考答案**

（55）C

**试题（56）**

把下列 8 个地址块 20.15.0.0～20.15.7.0 聚合成一个超级地址块，则得到的网络地址是（56）。

（56）A．20.15.0.0/20　　B．20.15.0.0/21

C．20.15.0.0/16　　D．20.15.0.0/24

**试题（56）分析**

8 个地址块 20.15.0.0～20.15.7.0 的二进制形式分别是：

地址块 20.15.0.0 的二进制是：　**00010100.00001111. 00000**000.00000000

地址块 20.15.1.0 的二进制是：　**00010100.00001111. 00000**001.00000000

地址块 20.15.2.0 的二进制是：　**00010100.00001111. 00000**010.00000000

地址块 20.15.3.0 的二进制是：　**00010100.00001111. 00000**011.00000000

地址块 20.15.4.0 的二进制是：　**00010100.00001111. 00000**100.00000000

地址块 20.15.5.0 的二进制是：　**00010100.00001111. 00000**101.00000000

地址块 20.15.6.0 的二进制是：　**00010100.00001111. 00000**110.00000000

地址块 20.15.7.0 的二进制是：　**00010100.00001111. 00000**111.00000000

可见，地址掩码可以设为 21 位，8 个地块组成的超网是 20.15.0.0/21。

**参考答案**

（56）B

**试题（57）**

每一个访问控制列表（ACL）最后隐含着一条语句＿（57）＿。

（57）A．deny any　　　　B．deny all

C．permit any　　　　D．permit all

**试题（57）分析**

出于安全性考虑，ACL的默认动作是拒绝（Implicit Deny），即在ACL中没有找到匹配的语句时分组将被拒绝通过，这相当于在列表最后有一个隐含语句拒绝了所有的通信（deny any）。由此引申出的一条规则是：每一个ACL至少要有一条“允许”语句，否则只有“拒绝”语句的ACL将丢弃所有的分组。

**参考答案**

（57）A

**试题（58）**

关于访问控制列表，下面的论述中错误的是＿（58）＿。

（58）A．访问控制列表要在路由器全局模式下配置

B．具有严格限制条件的语句应放在访问控制列表的最后

C．每一个有效的访问控制列表至少应包含一条允许语句

D．访问控制列表不能过滤由路由器自己产生的数据

**试题（58）分析**

当一个分组经过时，路由器按照一定的步骤找出与分组信息匹配的ACL语句对其进行处理。路由器自顶向下逐个处理ACL语句，首先把第一个语句与分组信息进行比较，如果匹配，则路由器将允许（Permit）或拒绝（Deny）分组通过；如果第一个语句不匹配，则照样处理第二个语句，直到找出一个匹配的。如果在整个列表中没有发现匹配的语句，则路由器丢弃该分组。于是，可以对ACL语句的处理规则总结出以下要点：

① 一旦发现匹配的语句，就不再处理列表中的其他语句。

② 语句的排列顺序很重要。

③ 如果整个列表中没有匹配的语句，则分组被丢弃。

需要特别强调ACL语句的排列顺序。如果有两条语句，一个拒绝来自某个主机的通信，另一个允许来自该主机的通信，则排在前面的语句将被执行，而排在后面的语句将被忽略。所以在安排ACL语句的顺序时要把最特殊的语句排在列表的最前面，而最一般的语句排在列表的最后面，这是ACL语句排列的基本原则。例如下面的两条语句组成一个标准ACL。

```
access-list 10 permit host 172.16.1.0 0.0.0.255
access-list 10 deny host 172.16.1.1
```

第一条语句表示允许来自子网 172.16.1.0/24 的所有分组通过，而第二条语句表示拒绝来自主机 172.16.1.1 的通信。如果路由器收到一个源地址为 172.16.1.1 的分组，则首先与第一条语句进行匹配，该分组被允许通过，第二条语句就被忽略了。要达到预想的结果——允许来自除主机 172.16.1.1 之外的、属于子网 172.16.1.0/24 的所有通信，则两条语句的顺序必须互换。

access-list 10 deny host 172.16.1.1

access-list 10 permit host 172.16.1.0 0.0.0.255

可见，列表顶上是特殊性语句，列表底部是一般性语句。

**参考答案**

（58）B

**试题（59）、（60）**

IPv6 的可聚合全球单播地址前缀为__（59）__，任意播地址的组成是__（60）__。

（59）A．010　　B．011　　C．001　　D．100

（60）A．子网前缀+全 0　　B．子网前缀+全 1

C．链路本地地址前缀+全 0　　D．链路本地地址前缀+全 1

**试题（59）、（60）分析**

IPv6 地址扩展到 128 位。$2^{128}$ 足够大，这个地址空间可能永远用不完。IPv6 地址采用冒号分隔的十六进制数表示，例如下面是一个 IPv6 地址

8000:0000:0000:0000:0123:4567:89AB:CDEF

IPv6 地址的格式前缀（Format Prefix，FP）用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可表示为“IPv6 地址/前缀长度”的形式。例如 60 位的地址前缀 12AB00000000CD3，有下列几种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

IPv6 地址格式前缀的初始分配如下表所示。

**表　IPv6 地址的初始分配**

| 分　　配 | 前缀（二进制） | 占地址空间的比例 |
|---|---|---|
| 保留 | 0000 0000 | 1/256 |
| 未分配 | 0000 000 | 11/256 |
| 为 NSAP 地址保留 | 0000 001 | 1/128 |
| 为 IPX 地址保留 | 0000 010 | 1/128 |
| 未分配 | 0000 011 | 1/128 |
| 未分配 | 0000 1 | 1/32 |
| 未分配 | 0001 | 1/16 |

续表

| 分　　配 | 前缀（二进制） | 占地址空间的比例 |
|---|---|---|
| 可聚合全球单播地址 | 001 | 1/8 |
| 未分配 | 010 | 1/8 |
| 未分配 | 011 | 1/8 |
| 未分配 | 100 | 1/8 |
| 未分配 | 101 | 1/8 |
| 未分配 | 110 | 1/8 |
| 未分配 | 1110 | 1/16 |
| 未分配 | 1111 0 | 1/32 |
| 未分配 | 1111 10 | 1/64 |
| 未分配 | 1111 110 | 1/128 |
| 未分配 | 1111 1110 0 | 1/512 |
| 链路本地单播地址 | 1111 1110 10 | 1/1024 |
| 站点本地单播地址 | 1111 1110 11 | 1/1024 |
| 组播地址 | 1111 1111 | 1/256 |

任意播地址仅用做目标地址，且只能分配给路由器。任意播地址是在单播地址空间中分配的。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。为构造一个子网-路由器任意播地址，子网前缀必须固定，其余位置全“0”，见下图。

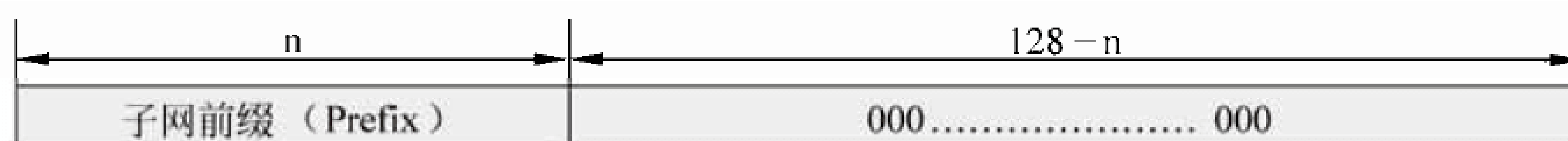



图　子网-路由器任意播地址

**参考答案**

（59）C　（60）A

**试题（61）**

如果一个 TCP 连接处于 ESTABLISHED 状态，这是表示<u>（61）</u>。

（61）A. 已经发出了连接请求

B. 连接已经建立

C. 处于连接监听状态

D. 等待对方的释放连接响应

**试题（61）分析**

下图所示为 TCP 的连接状态图。事实上，在 TCP 协议运行过程中，有多个连接处于不同的状态。

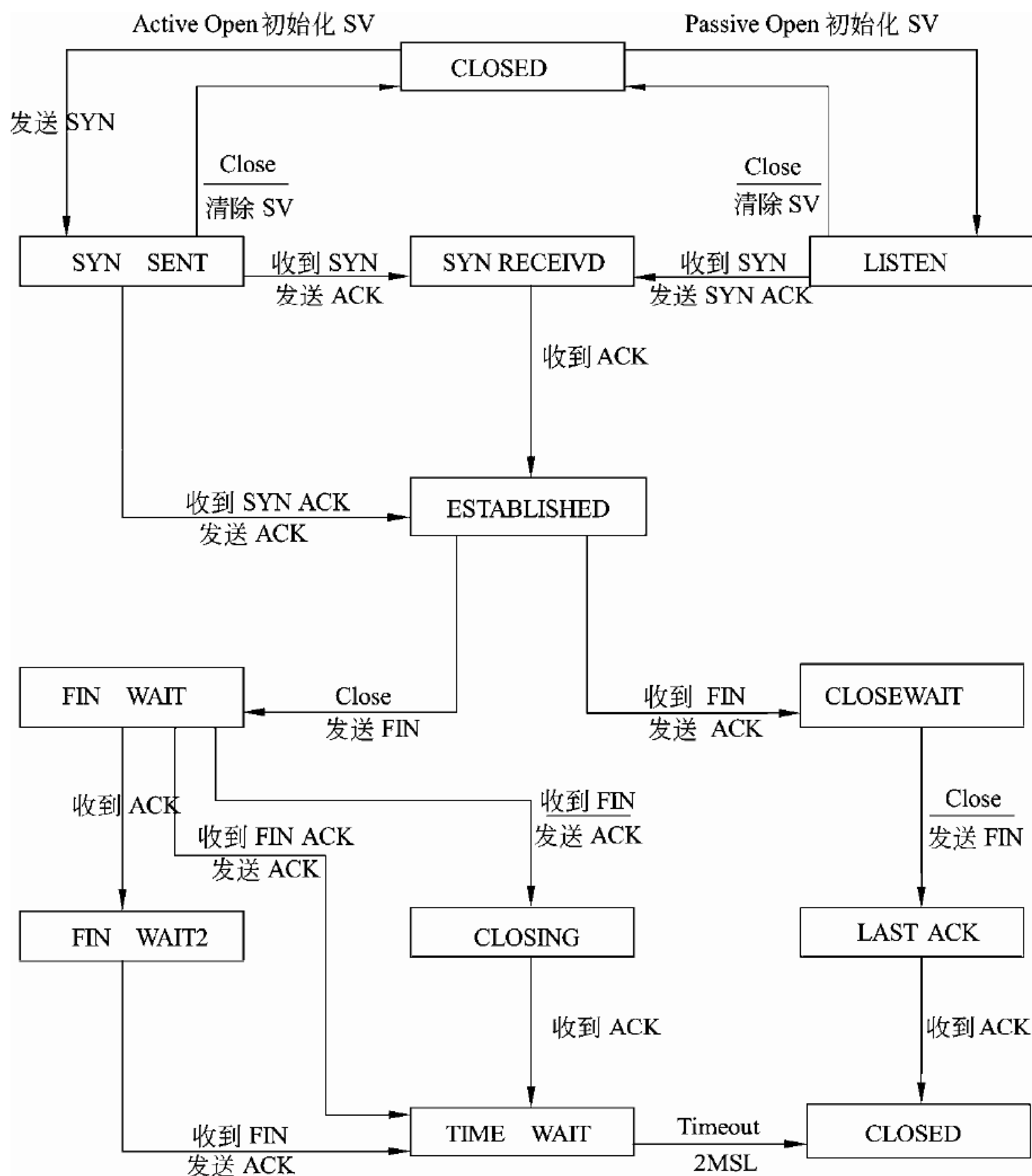



图　TCP 连接状态图

由图可知，如果一个 TCP 连接处于 ESTABLISHED 状态，则表示连接已经建立。

**参考答案**

（61）B

**试题（62）**

以太网采用的 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，关于这个算法，下面的论述中错误的是__（62）__。

（62）A．冲突次数越多，后退的时间越短

B．平均后退次数的多少与负载大小有关

C．后退时延的平均值与负载大小有关

D. 重发次数达到一定极限后放弃发送

**试题（62）分析**

以太网采用的 CSMA/CD 协议，当冲突发生时要通过二进制指数后退算法计算后退时延，退一段时间重新发送。后退时间的多少对网络的稳定工作有很大影响。特别是在负载很重的情况下，为了避免很多站连续发生冲突，需要设计有效的后退算法。按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。或者说，随着重发次数 n 的增加，后退时延 $t_\xi$的取值范围按 2 的指数增大。即第一次试发送时 n 的值为 0，每冲突一次 n 的值加 1，并按下式计算后退时延。

$$\begin{cases} \xi = \text{random}[0,2^n] \\ t_\xi = \xi\tau \end{cases}$$

其中，第一式是在区间[0，$2^n$]中取一均匀分布的随机整数$\xi$，第二式是计算出随机后退时延。为了避免无限制的重发，要对重发次数 $n$ 进行限制，这种情况往往是信道故障引起的。通常当 $n$ 增加到某一最大值（例如 16）时，停止发送，并向上层协议报告发送错误。

当然，还可以有其他的后退算法，但二进制指数后退算法考虑了网络负载的变化情况。事实上，后退次数的多少往往与负载大小有关，二进制指数后退算法的优点正是把后退时延的平均取值与负载的大小联系起来了。

**参考答案**

（62）A

**试题（63）**

在局域网中可动态或静态划分 VLAN，静态划分 VLAN 是根据__（63）__划分。

（63）A. MAC 地址　　　　B. IP 地址
　　　C. 端口号　　　　　D. 管理区域

**试题（63）分析**

虚拟局域网 VLAN 是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络。虚拟局域网与物理局域网具有同样的属性，然而其中的工作站可以不属于同一物理网段。任何交换端口都可以分配给某个 VLAN，属于同一个 VLAN 的所有端口构成一个广播域。每一个 VLAN 是一个逻辑网络，发往 VLAN 之外的分组必须通过路由器进行转发。

在交换机上实现 VLAN，可以采用静态的或动态的方法。

① 静态分配 VLAN。为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口所在的 VLAN。

② 动态分配 VLAN。动态 VLAN 通过网络管理软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址

划分 VLAN 的方法应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的什么地方，接入交换机根据设备的 MAC 地址就可以确定该设备的 VLAN 成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的 VLAN。但是当用户数量很多时，对每个用户设备分配 VLAN 的工作量是很大的管理负担。

**参考答案**

（63）C

**试题（64）**

在 IEEE 802.11 无线局域网中使用的通信技术有多种，但是不包括__（64）__。

（64）A．FHSS　　B．DSSS
　　　C．CDMA　　D．IR

**试题（64）分析**

无线网主要使用 3 种通信技术：红外线、扩展频谱和窄带微波技术。

（1）红外通信。

红外线（Infrared Ray，IR）通信技术可以用来建立 WLAN。IR 通信分为 3 种技术：

① 定向红外光束：用于点对点链路，可以连接几座大楼中的网络，每幢大楼的路由器或网桥在视距范围内通过 IR 收发器互相连接。

② 全方向广播红外线：基站置于天花板上，基站上的发射器向各个方向广播信号，所有终端的 IR 收发器都用定位光束瞄准天花板上的基站，可以接收基站发出的信号，或向基站发送信号。

③ 漫反射红外线：在这种配置中，所有的发射器都集中瞄准天花板上的一点。红外线射到天花板上后被全方位地漫反射回来，并被房间内所有的接收器接收。

（2）扩展频谱通信。

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（FHSS），更新的版本是直接序列扩展频谱（DSSS），这两种技术在 IEEE 802.11 定义的 WLAN 中都有应用。

（3）窄带微波通信。

窄带微波（Narrowband Microwave）是指使用微波无线电频带（RF）进行数据传输，其带宽刚好能容纳传输信号。以前所有的窄带微波无线网产品都需要申请许可证，现在已经出现了 ISM 频带内的窄带微波无线网产品。

**参考答案**

（64）C

**试题（65）**

ZigBee 网络是 IEEE 802.15.4 定义的低速无线个人网，其中包含全功能和简单功能两类设备，下面关于这两类设备的描述中错误的是__（65）__。

（65）A．协调器是一种全功能设备，只能作为 PAN 的控制器使用
B．被动式红外传感器是一种简单功能设备，接受协调器的控制
C．协调器也可以运行某些应用，发起和接受其他设备的通信请求
D．简单功能设备之间不能互相通信，只能与协调器通信

**试题（65）分析**

IEEE 802.15.4 标准定义的低速无线个人网（Low Rate-WPAN）包含两类设备：全功能设备（Full-Function Device，FFD）和简单功能设备（Reduced-Function Device，RFD）。FFD 有 3 种工作模式，可以作为一般的设备、协调器（coordinator）或 PAN 协调器，而 RFD 功能简单，只能作为设备使用，例如电灯开关、被动式红外传感器等。这些设备不需要发送大量的信息，通常接受某个 FFD 的控制。FFD 可以与 RFD 或其他 FFD 通信，而 RFD 只能与 FFD 通信，RFD 之间不能互相通信。

**参考答案**

（65）A

**试题（66）**

在 IPv4 和 IPv6 混合的网络中，协议翻译技术用于__（66）__。

（66）A．两个 IPv6 主机通过 IPv4 网络通信
B．两个 IPv4 主机通过 IPv6 网络通信
C．纯 IPv4 主机和纯 IPv6 主机之间的通信
D．两个双协议栈主机之间的通信

**试题（66）分析**

协议翻译技术用于纯 IPv6 主机与纯 IPv4 主机之间的通信。已经提出了多种翻译方法。例如 RFC 2765 定义的无状态 IP/ICMP 翻译（Stateless IP/ICMP Translation， SIIT）。这种技术类似于 IPv4 中的 NAT-PT 技术，但它并不是为 IPv6 主机动态地分配 IPv4 地址。SIIT 转换器规范描述了从 IPv6 到 IPv4 的协议转换机制，包括 IP 头的翻译方法以及 ICMP 报文的翻译方法等。当 IPv6 主机发出的分组到达 SIIT 转换器时，IPv6 分组头被翻译为 IPv4 分组头，分组的源地址采用 IPv4 翻译地址，目标地址采用 IPv4 映射地址，然后这个分组就可以在 IPv4 网络中传送了。

RFC 2766 定义了协议翻译方法 NAT-PT（Network Address Translator – Protocol Translator），也可以用于纯 IPv6 主机与纯 IPv4 主机之间的通信。实现 NAT-PT 技术必须指定一个服务器作为 NAT-PT 网关，并且要准备一个 IPv4 地址块作为地址翻译之用，要为每个站点至少预留一个 IPv4 地址。与 SIIT 不同，RFC 2766 定义的是有状态的翻译技术，即要记录和保持会话状态，按照会话状态参数对分组进行翻译，包括对 IP 地址及其相关的字段（例如 IP、TCP、UDP、ICMP 等）进行翻译。

协议翻译技术适用于 IPv6 孤岛与 IPv4 海洋之间的通信。这种技术要求一次会话中的双向数据包都在同一个路由器上完成转换，所以它只能适用于同一路由器连接的网络。

这种技术的优点是不需要进行 IPv4 和 IPv6 终端的升级改造，只要求在 IPv4 和 IPv6 之间的网络转换设备上启用 NAT-PT 功能就可以了。但是实现这种技术时，一些协议字段在转换时仍不能完全保持原有的含义，并且缺乏端到端的安全性。

**参考答案**

（66）C

**试题（67）、（68）**

结构化布线系统分为六个子系统，其中水平子系统的作用是__（67）__，园区子系统的作用是__（68）__。

（67）A．连接各个建筑物中的通信系统

B．连接干线子系统和用户工作区

C．实现中央主配线架与各种不同设备之间的连接

D．实现各楼层设备间子系统之间的互连

（68）A．连接各个建筑物中的通信系统

B．连接干线子系统和用户工作区

C．实现中央主配线架与各种不同设备之间的连接

D．实现各楼层设备间子系统之间的互连

**试题（67）、（68）分析**

结构化布线系统分为 6 个子系统。

① 工作区子系统（Work Location）。

工作区子系统是指从终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区。工作区应支持电话、数据终端、计算机、电视机、监视器以及传感器等多种终端设备。

② 水平布线子系统（Horizontal）。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平子系统的作用是将干线子系统线路延伸到用户工作区。

③ 管理子系统（Administration）。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。

④ 干线子系统（Backbone）。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。

⑤ 设备间子系统（Equipment）。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交

换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如PBX、网络设备和监控设备等）之间的连接。

⑥ 建筑群子系统（Campus）。

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。大楼之间的布线方法有三种：一种是地下管道敷设方式；第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志；最后一种是架空明线，这种方法需要经常维护。

**参考答案**

（67）B （68）A

**试题（69）**

网络系统设计过程中，逻辑网络设计阶段的任务是<u>（69）</u>。

（69）A．对现有网络资源进行分析，确定网络的逻辑结构

B．根据需求说明书确定网络的安全系统结构

C．根据需求规范和通信规范，分析各个网段的通信流量

D．根据用户的需求，选择特定的网络技术、网络互连设备和拓扑结构

**试题（69）分析**

网络的逻辑结构设计来自于用户需求中描述的网络行为和性能等要求。逻辑设计要根据网络用户的分类和分布，选择特定的网络技术，形成特定的网络结构。网络结构大致描述了设备的互联及分布，但是不对具体的物理位置和运行环境进行确定。

**参考答案**

（69）D

**试题（70）**

下列关于网络汇聚层的描述中，正确的是<u>（70）</u>。

（70）A．要负责收集用户信息，例如用户IP 地址、访问日志等

B．实现资源访问控制和流量控制等功能

C．将分组从一个区域高速地转发到另一个区域

D．提供一部分管理功能，例如认证和计费管理等

**试题（70）分析**

大型局域网可以划分为多个层次，层次化模型中最典型的是三层模型，这种模型允许在三个路由或交换层次上实现流量汇聚和分组过滤功能。三层模型将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用。核心层提供不同区域之间的最佳路由和高速数据传送；汇聚层将网络业务连接到接入层，并且实施与安全、流量、负载和路由相关的策略；接入层为用户提供了在本地网段访问应用系统的能力，还要解决相邻用户之间的互访需要，接入层要负责一些用户信息（例如用户IP 地址、MAC地址和访问日志等）的收集工作和用户管理功能（包括认证和计费等）。

**参考答案**

（70）B

**试题（71）～（75）**

CDMA for cellular systems can be described as follows. As with FDMA, each cell is allocated a frequency （71）, which is split into two parts, half for reverse (mobile unit to base station) and half for （72） (base station to mobile unit). For full-duplex （73）, a mobile unit uses both reverse and forward channels. Transmission is in the form of direct-sequence spread （74）, which uses a chipping code to increase the data rate of the transmission, resulting in an increased signal bandwidth. Multiple access is provided by assigning （75） chipping codes to multiple users, so that the receiver can recover the transmission of an individual unit from multiple transmissions.

（71）A. wave　B. signal　C. bandwidth　D. domain

（72）A. forward　B. reverse　C. backward　D. ahead

（73）A. connection　B. transmission　C. compromise　D. communication

（74）A. structure　B. spectrum　C. stream　D. strategy

（75）A. concurrent　B. orthogonal　C. higher　D. lower

**参考译文**

用于蜂窝系统的 CDMA 技术可以描述如下。就像 FDMA 一样，每一个小区被分配了一个频带，该频带划分为两半，一半用于反向信道（从移动终端到基站），一半用于正向信道（从基站到移动终端）。在全双工通信中，移动终端使用了反向和正向两个信道。传输以直接序列扩频方式进行，用一个码片来增加传输的数据速率，同时也产生了额外的信号带宽。通过把正交的各个码片指定给不同的用户就可以实现多路访问，这样接收者就能够从多个传输中提取并恢复需要的传输单元。

**参考答案**

（71）C　（72）A　（73）D　（74）B　（75）B

# 第 24 章　2014 下半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业的网络结构如图 1-1 所示。

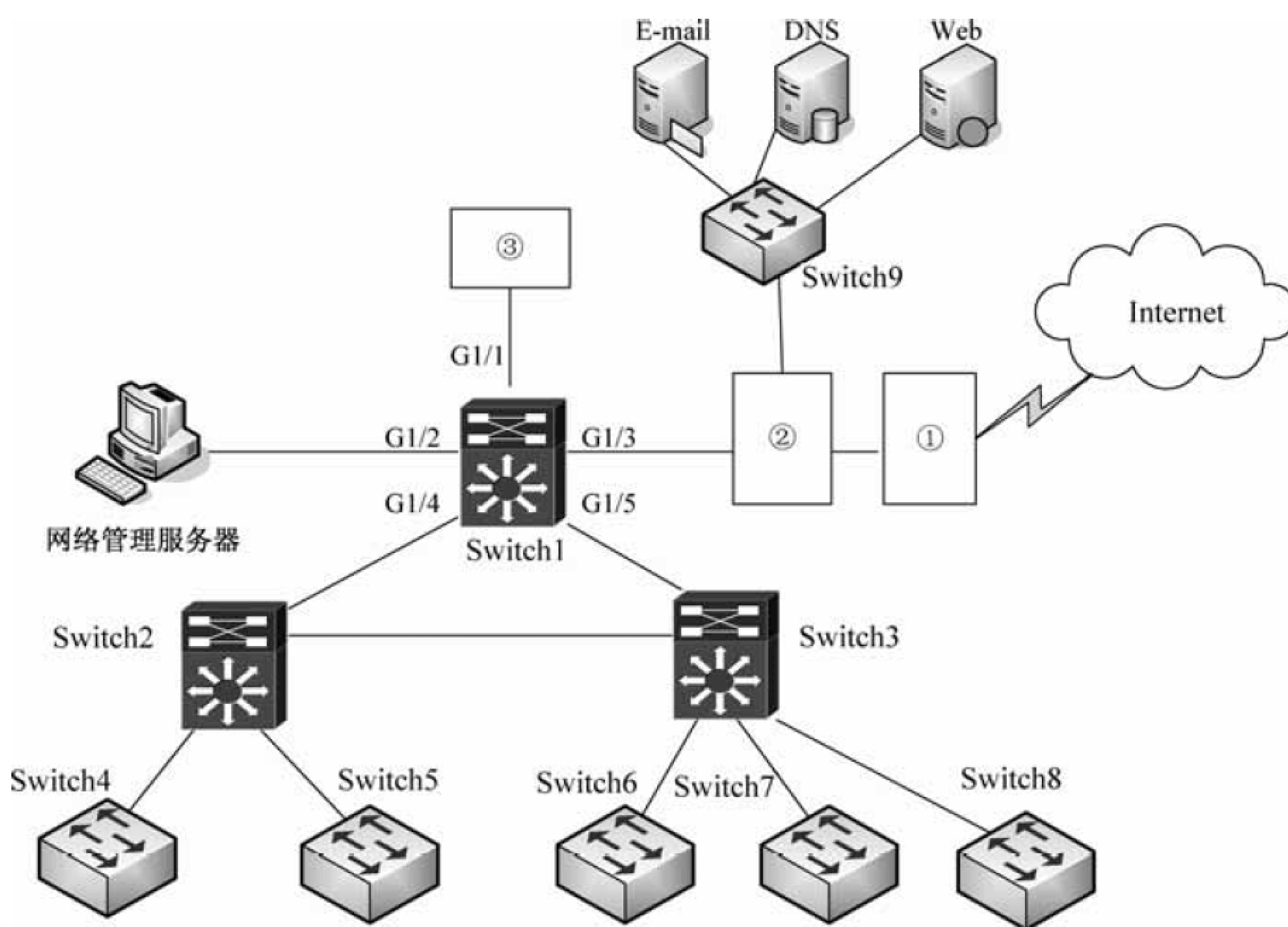



图 1-1

**【问题 1】（6 分）**

1．图 1-1 中的网络设备①应为___（1）___，网络设备②应为___（2）___，从网络安全的角度出发，Switch9 所组成的网络一般称为___（3）___区。

2．图 1-1 中③处的网络设备的作用是检测流经内网的信息，提供对网络系统的安全保护。该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为___（4）___，其连接的 Switch1 的 G1/1 端口称为___（5）___端口，这种连接方式一般称为___（6）___。

【问题 2】（5 分）

1．随着企业用户的增加，要求部署上网行为管理设备对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在图 1-1 中的＿（7）＿和＿（8）＿之间比较合理。

2．网卡的工作模式有直接、广播、多播和混杂四种模式，缺省的工作模式为＿（9）＿和＿（10）＿，即它只接收广播帧和发给自己的帧。网络管理机通常在用抓包工具时，需要把网卡置于＿（11）＿，这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【问题 3】（5 分）

针对图 1-1 中的网络结构，各台交换机需要运行＿（12）＿协议，以建立一个无环路的树状网络结构。默认情况下，该协议的优先级值为＿（13）＿。在该协议中，根交换机是根据＿（14）＿来选择的，值小的为根交换机；如果相同，再比较＿（15）＿。

当图 1-1 中的 Switch1～Switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 Switch1～Switch8 上使用＿（16）＿功能。

【问题 4】（4 分）

根据层次化网络的设计原则，从图 1-1 中可以看出该企业网络采用了由＿（17）＿层和＿（18）＿层组成的两层架构，其中 MAC 地址过滤和 IP 地址绑定等功能是由＿（19）＿完成的，分组的高速转发是由＿（20）＿完成的。

**试题一分析**

本题考查网络规划设计方面的相关知识。

【问题 1】

本问题主要考查网络拓扑结构。

路由器具有广域网互联、隔离广播信息和异构网络互连等能力，是企业网建设和互联网络建设中必不可少的设备。从图中的网络拓扑结构可知，设备（1）处于该企业网和 Internet 之间，因此需要使用路由器进行互联，以实现该企业网路由信息的边界计算网络地址转换等功能。

通常 Internet 是一个不可信任的网络，而企业内部网络要求是一个可信任的网络。因此设备（2）需要部署防火墙设备，从而保护内部网络资源不会被外部非授权用户使用，防止内部网络受到外部非法用户的攻击。防火墙一般按照防护的区域可分为信任区、非信任区以及 DMZ 区。其中 DMZ 区是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、Mail 服务器和 DNS 等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方

案，对攻击者来说又多了一道关卡。

入侵防护系统（IPS）兼有防火墙、IDS 和防病毒等安全组件的特性，当数据包经过时将对其进行过滤检测，以确保该数据包是否含有威胁网络安全的特征。如果检测到一个恶意的数据包，系统不但发出警报，还将采取相应措施阻断攻击。图中设备（3）直接接在交换机 1 的 G1/1 接口上（此接口为镜像端口），用于检测、分析和处理从设备（2）进入交换机 1 的数据包。根据网络拓扑结构和安全要求的不同，IPS 可以通过旁路接入或者直接串接等方式部署在被检测的网络中。

**【问题 2】**

本问题主要考查上网行为管理设备和网卡的工作模式。

上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计和用户行为分析。通过对上网行为管理的需求进行分析，根据图中的网络拓扑结构，可以得出该设备应该部署在交换机 1 和设备（2）之间，这样才能满足企业的要求。

网卡具有如下的四种工作模式：

（1）广播模式（Broad Cast Model）：物理地址（MAC）是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

（2）多播传送（MultiCast Model）：多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

（3）直接模式（Direct Model）：工作在直接模式下的网卡只接收目的地址是自己 Mac 地址的帧。

（4）混杂模式（Promiscuous Model）：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接收同一网络内所有站点所发送的数据包，这样就可以达到对网络信息监视捕获的目的。

**【问题 3】**

本问题主要考查生成树协议。

生成树协议（STP）是一个数据链路层的协议。其基本原理是通过在交换机之间传递一种特殊的协议报文，网桥协议数据单元（Bridge Protocol Data Unit，简称 BPDU），来确定网络的拓扑结构。BPDU 有两种：配置 BPDU（Configuration BPDU）和 TCN BPDU。前者是用于计算无环的生成树的，后者则是用于在二层网络拓扑发生变化时产生用来缩短 CAM 表项的刷新时间的（由默认的 300s 缩短为 15s）。Spanning Tree Protocol（STP）在 IEEE 802.1D 文档中定义。该协议的原理是按照树的结构来构造网络拓扑，消除网络中的环路，避免由于环路的存在而造成广播风暴问题。在该协议中，交换机是根据交换

机优先级来选择的，值小的为根交换机。如果相同，再比较 MAC 地址。交换机优先级是一个十进制数，用来在生成树算法中衡量一个交换机的优先度，其值的范围是 0～65535，默认情况下，其值为 32768。

BackboneFast 是对 UplinkFast 的一种补充，UplinkFast 能够检测直连链路的失效，BackboneFast 是用来检测间接链路的失效。当启用了 BackboneFast 的交换机检测到间接链路失效之后，会马上使阻塞的端口进入监听状态，少了 20s 的老化时间。如果要启用 BackboneFast 特性，应该在网络中的所有交换机上都启用。

【问题 4】

本问题主要考查网络分层概念。

图中所示的网络拓扑结构采用了核心层和接入层的两层架构理念。其中，由交换机 1～交换机 3 组成核心层，主要完成的功能有：分组的高速转发；汇聚下一层的用户流量，进行数据分组传输的汇聚、转发和交换；根据接入层的用户流量，进行本地路由、数据包过滤、协议转换、流量均衡、QoS 优先级管理以及安全控制、IP 地址转换、流量整型等处理。由交换机 4～交换机 8 组成了接入层，主要完成的功能是：为用户提供了在本地网段访问应用系统的能力，解决相邻用户之间互相访问的需求，并且为这些访问提供足够的带宽；适当地负责部分用户管理功能（如 MAC 层过滤、IP 地址绑定、用户认证、计费管理等）；负责部分用户信息收集工作（如用户的 IP 地址、MAC 地址、访问日志等）。

**参考答案**

【问题 1】

（1）路由器

（2）防火墙或其他具有类似功能的网络安全设备

（3）非军事/DMZ

（4）IPS（入侵防御系统）或 IDS（入侵检测系统）

（5）镜像

（6）旁路方式

【问题 2】

（7）主交换机或 Switch1　——（7）和（8）答案可互换

（8）防火墙或网络设备②　——（7）和（8）答案可互换

（9）广播模式　——（9）和（10）答案可互换

（10）直接模式　——（9）和（10）答案可互换

（11）混杂模式

【问题 3】

（12）STP 或生成树

（13）32768

（14）交换机优先级

（15）MAC 地址

（16）BackboneFast

**【问题 4】**

（17）核心

（18）接入

（19）Switch4～Switch8 或 接入层交换机

（20）Switch1～Switch3 或 核心层交换机

**试题二（共 20 分）**

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

**【说明】**

某中学为两个学生课外兴趣小组提供了建立网站的软硬件环境。网站环境的基本配置方案如下：

1．两个网站配置在同一台服务器上，网站服务由 Win 2003 环境下的 IIS 6.0 提供；

2．网站的管理通过 Win 2003 的远程桌面实现，并启用 Win 2003 的防火墙组件；

3．为兴趣小组建立各自独立的文件夹作为上传目录和网站的主目录，对用户使用磁盘空间大小进行了设定；

4．通过不同的域名分别访问课外兴趣小组各自的网站。

按照方案，学校的网络工程师安装了 Win 2003 服务器，使用 IIS 6.0 建立 Web 和 FTP 服务器，配置了远程桌面管理、防火墙，在服务器上为两个课外兴趣小组分配了不同的用户名，进行了初步的权限配置。

**【问题 1】（4 分）**

Win 2003 远程桌面服务的默认端口是__（1）__，对外提供服务使用__（2）__协议。在图 2-1 中，若要拒绝外部设备 PING 服务器，在防火墙的 ICMP 配置界面上应该如何操作？

**【问题 2】（4 分）**

1．在图 2-2 中，Web 服务扩展选项中“所有未知 CGI 扩展 禁止”的含义是什么？

2．在图 2-2 中，如何配置 Web 服务扩展，网站才能提供对 ASP.NET 或 ASP 程序的支持。

**【问题 3】（5 分）**

在图 2-2 中，选择 IIS 管理器中的 FTP 站点→新建→虚拟目录，分别设置 FTP 用户与__（3）__、__（4）__的对应关系。

由于 IIS 内置的 FTP 服务不支持__（5）__，所以 FTP 用户密码是以明文方式在网络上传输，安全性较弱。

**【问题 4】（4 分）**

在 IIS 6.0 中，每个 Web 站点都具有唯一的、由三部分组成的标识符，用来接收和

响应请求，分别是 （6） 、 （7） 和 （8） 。网络工程师通过点击网站属性→网站→高级选项，通过添加 （9） 的方式在一个 IP 地址上建立多个网站。

**【问题 5】（3 分）**

在 （10） 文件系统下，为了预防用户无限制的使用磁盘空间，可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是 （11） 和 （12） 。

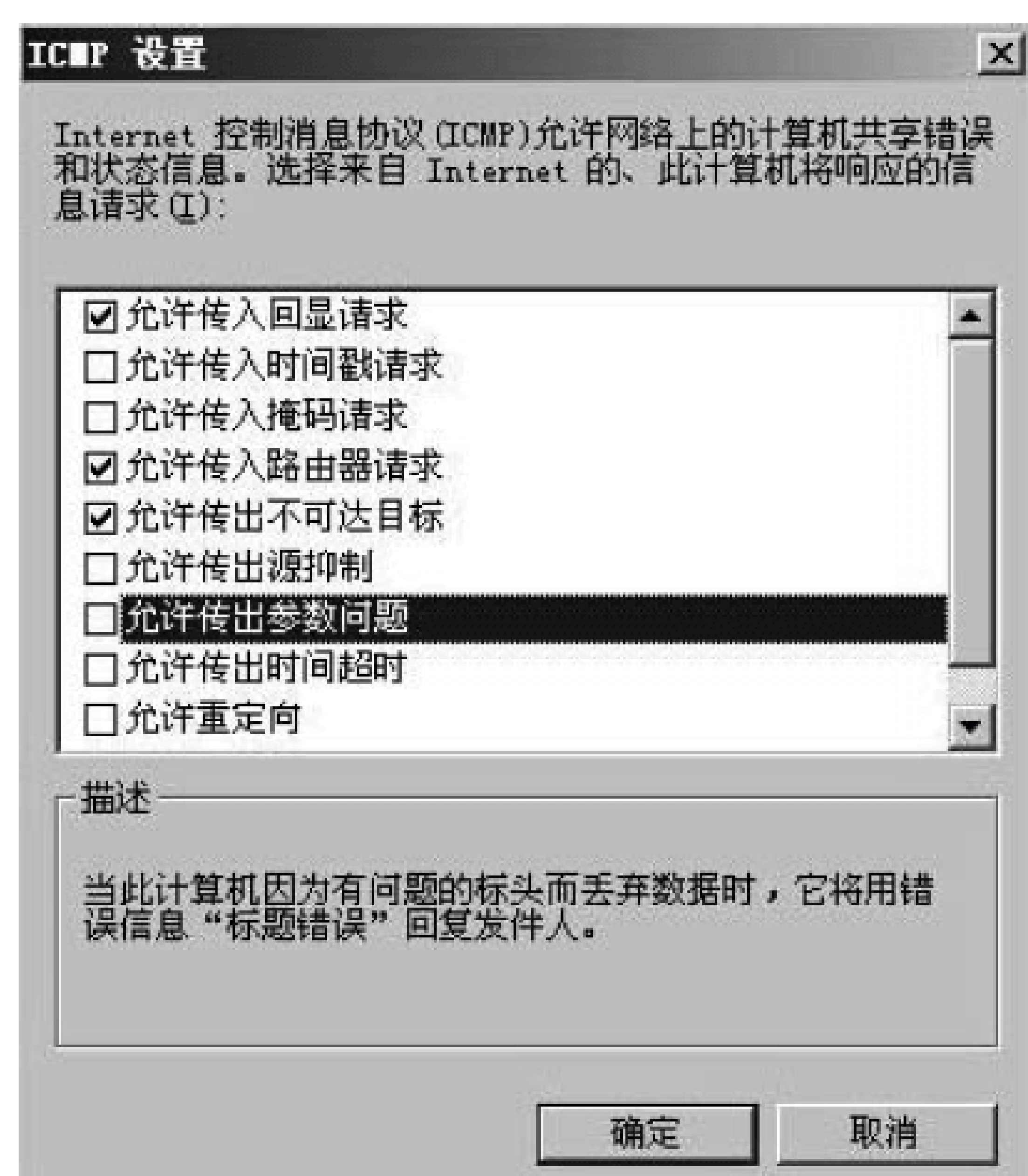



图 2-1




图 2-2

## 试题二分析

本题考查 Win 2003 服务器配置的相关知识。

**【问题 1】**

远程桌面是方便 Windows 服务器管理员对服务器进行基于图形界面的远程管理的工具。远程桌面是基于 RDP（RemoteDesktopProtocol 远程桌面协议）的多通道（multi-channel）协议，让使用者（所在计算机称为用户端或“本地计算机”）连上提供服务器或“远程计算机”，远程桌面默认使用的端口是 3389。

ICMP 协议是一种用于传输出错报告控制信息，对于网络安全具有极其重要的意义。它是 TCP/IP 协议簇的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标，IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。

**【问题 2】**

如果选择允许所有通用网关接口（CGI）在 Web 服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在 IIS 6.0 上运行，否则它就不能运行。

要想网站提供对 ASP.NET 或 ASP 程序的支持，必须增加 ASP.NET 模块（启用 ASP.NET 的服务扩展项）。将 Active Server Pages 配置为“允许”，IIS 6.0 即可提供对 ASP

支持。

【问题3】

FTP（File Transfer Protocol，FTP）是TCP/IP网络上两台计算机传送文件的协议，FTP是在TCP/IP网络和Internet上最早使用的协议之一，它属于网络协议的应用层。FTP客户机可以给服务器发出命令来下载文件、上传文件、创建或改变服务器上的目录，FTP的默认端口是21。由于IIS中的FTP服务不支持安全套接字层（SSL）上的 FTP，因此，如果要保证通信的安全性，同时又需要使用 FTP 作为传输协议（相对于在 SSL 上使用 WebDAV 而言），可以考虑在加密通道（如虚拟专用网络）上使用 FTP，此类加密通道通过点对点隧道协议或 IPSec 保证安全性。

【问题4】

IIS是一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。IIS 6.0增强了安全性，为了尽量减少系统被攻击的危险，在默认情况下IIS 6.0是不会被安装在Win 2003中的，管理员需要手动进行安装，IIS 6.0在被锁定状态中只为静态内容（.htm，.jpg，.bmp等等）提供服务，通过网络服务扩展节点，网站管理员可根据企业的需求起用或禁止IIS功能。

【问题5】

在NTFS文件系统下，为了预防用户无限制的使用磁盘空间，可以使用磁盘配额管理。启动磁盘配额时，设置的两个参数分别是磁盘配额限制和磁盘配额警告级别。

参考答案

【问题1】

（1）3389

（2）RDP

不勾选“允许传入回显请求”

【问题2】

1．如果选择允许所有通用网关接口（CGI）在Web服务器上运行，则 Web 服务器容易受到使用 CGI 技术的计算机病毒或蠕虫程序的攻击。禁止该扩展意味着除非明确地允许一个应用在IIS 6.0上运行，否则它就不能运行。

2．增加ASP.NET模块（启用ASP.NET的服务扩展项），网站才能提供对ASP.NET的支持。将Active Server Pages 配置为“允许”，IIS 6.0即可提供对ASP支持。

【问题3】

（3）别名

（4）目录名

（5）SSL

【问题4】

（6）IP地址

（7）端口号

（8）主机头名

（9）主机头名

**【问题 5】**

（10）NTFS

（11）磁盘配额限制

（12）磁盘配额警告级别

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业的网络结构如图 3-1 所示。

图 3-1　企业网络拓扑结构

按照网络拓扑结构为该企业网络进行网络地址配置，地址分配如表 3-1 所示。

**表 3-1　网络地址分配表**

| 设　　备 | 地　　址 |
|---|---|
| Router-NAT | F0/1:192.168.1.1/24<br>S0:61.192.93.100/24<br>S1:202.102.100.100/24 |
| Web 服务器 | 192.168.1.100 |
| ISP-A | 61.192.93.200/24 |
| ISP-B | 202.102.100.200/24 |
| ISP-A 地址池 | 61.192.93.100~61.192.93.102 |
| ISP-B 地址池 | 202.102.100.100~202.102.100.102 |

**【问题 1】（4 分）**

企业网络中使用私有地址，如果内网用户要访问互联网，一般使用__（1）__技术将私有网络地址转换为公有地址。在使用该技术时，往往是用__（2）__技术指定允许转换的内部主机地址范围。

一般来说，企业内网服务器需要被外部用户访问，就必须对其做 NAT 转换，内部服务器映射的公共地址不能随意更换，需要使用__（3）__NAT 技术。但是对于企业内部用户来讲，使用一一映射的技术为每个员工配置一个地址很不现实，一般使用__（4）__NAT 技术以提高管理效率。

**【问题 2】（7 分）**

一般企业用户可能存在于任何一家运营商的网络中，为了确保每个运营商网络中的客户都可以高效地访问本企业所提供的网络服务，企业有必要同时接入多个运营商网络。根据企业网络的拓扑图和网络地址规划表，实现该企业出口 NAT 的双线接入。

首先，为内网用户配置 NAT 转换，其中以 61.192.93.0/24 代表 ISP-A 所有网段；其次为外网用户访问内网服务器配置 NAT 转换。根据需求，完成以下 Route-NAT 的部分配置命令。

```
…
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101__(5)__ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101______(6)______
//定义到达 ISP-B 所有网段的 ACL
Route-Switch(config)#ip nat pool ISP-A ____(7)____netmask 255.255.255.0
//定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B____(8)____netmask 255.255.255.0
//定义访问 ISP-B 的合法地址池
Route-Switch(config)#ip nat inside source list 100 pool ISP-A overload
Route-Switch(config)#ip nat inside source __________(9)__________
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
Route-Switch(config)# ip nat inside source static tcp ___(10)___extendable
//为内网 WEB 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)# ip nat inside source static tcp___(11)_extendable
//为内网 WEB 服务器配置 ISP-B 的静态 NAT 转换
…
```

**【问题 3】（6 分）**

在路由器的内部和外部接口启用 NAT，同时为了确保内网可以访问外部网络，在出口设备配置静态路由。根据需求，完成（或解释）Route-NAT 的部分配置命令。

```
…
Route-Switch(config)#int s0
Route-Switch(config)#_____(12)_____  //指定 NAT 的外部转换接口
Route-Switch(config)#int s1
```

```
Route-Switch(config)#___(13)___              //指定 NAT 的外部转换接口
Route-Switch(config)#int f0/1
Route-Switch(config)#___(14)___              //指定 NAT 的内部转换接口
Route-Switch(config)# ___(15)___        //配置到达 ISP-A 的流量从 s0 口转发
Route-Switch(config)#___(16)___            //配置默认路由指定从 s1 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s0 120  //___(17)___
…
```

**【问题 4】（3 分）**

常用的网络流量控制技术除了 ACL（访问控制列表）外还有 QoS（服务质量）。QoS 是网络的一种安全机制，主要用来解决网络延迟和阻塞等问题，它主要有三种工作模式，分别为＿＿（18）＿＿模型、Integrated service（或综合服务）模型及＿＿（19）＿＿模型，其中使用比较普遍的方式是＿＿（20）＿＿模型。

**试题三分析**

本题考查网络出口 NAT 的双线接入知识。

**【问题 1】**

本问题主要考查 NAT 转换的相关知识。

一般来说，由于企业内网大都使用私有网络地址，私有地址只能在局域网中使用，不能出现在互联网上，那么使用私有地址的内部主机想要访问互联网，就必须使用地址转换技术将其转换为公有地址，也就是说如果内网用户想要访问互联网，就必须使用 NAT 地址转换技术，将私有地址转换为在互联网应用的公有地址。在使用 NAT 地址转换技术时，往往要使用 ACL 技术来指定允许转换的内部主机地址范围。

根据映射的方式，可以将 NAT 技术分为静态 NAT 和动态 NAT。其中，静态 NAT 是手工配置的内部私有地址和外部公共地址的对应关系，除非人工修改，否则不会变化，一般对外发布服务器使用静态 NAT 技术。动态 NAT 是多个内部主机和外部公共地址随机对应的一种方式，主要是通过指定内部允许转换的地址范围和外部允许使用的地址范围，然后对两个范围映射。这样具体外部的一个公共地址被内部哪台主机使用不确定。主要适用于企业内网大量用户的客户端访问外网。

**【问题 2】**

本问题主要考查 ACL 和 PAT 的相关配置命令。

```
…
Route-Switch(config)#access-list 100 permit ip any 61.192.93.0 0.0.0.255
//定义到达 ISP-A 所有网段的 ACL
Route-Switch(config)#access-list 101 deny ip any 61.192.93.0 0.0.0.255
Route-Switch(config)#access-list 101 permit ip any any
//定义到达 ISP-B 所有网段的流量
//用的是排除 ISP-A 网段的方式进行定义，可以防止遗漏网段
Route-Switch(config)#ip nat pool ISP-A 61.192.93.100 61.192.93.102 netmask
```

```
255.255.255.0            //定义访问 ISP-A 的合法地址池
Route-Switch(config)#ip nat pool ISP-B 202.102.100.100 202.102.100.102
netmask 255.255.255.0            //定义访问 ISP-B 的合法地址池
Route-Switch(config)#ip nat inside source list 100 pool ISP-A overload
Route-Switch(config)#ip nat inside source list 101 pool ISP-B overload
//为内网用户实现区分目标运营商网络进行匹配的 NAT 转换
Route-Switch(config)# ip nat inside source static tcp 192.168.1.100 80
61.192.93.100 80____ extendable  //为内网 WEB 服务器配置 ISP-A 的静态 NAT 转换
Route-Switch(config)# ip nat inside source static tcp 192.168.1.100 80
202.102.100.100 80____   extendable //为内网 WEB 服务器配置 ISP-B 的静态 NAT 转换
```

**【问题 3】**

本问题主要考查 NAT 转换和默认路由的配置命令。

```
…
Route-Switch(config)#int s0                 //进入 s0 的子接口配置模式
Route-Switch(config)#ip nat outside         //指定 NAT 的外部转换接口
Route-Switch(config)#int s1                 //进入 s1 的子接口配置模式
Route-Switch(config)#ip nat outside         //指定 NAT 的外部转换接口
Route-Switch(config)#int f0/1               //进入 f0/1 的子接口配置模式
Route-Switch(config)#ip nat inside          //指定 NAT 的内部转换接口
Route-Switch(config)#ip route 61.192.93.0 255.255.255.0 s0     //配置到达
ISP-A 的流量从 s0 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s1          //配置默认路由
指定从 s1 口转发
Route-Switch(config)#ip route 0.0.0.0 0.0.0.0 s0 120      //配置备份路由，
或者配置浮动静态路由
…
```

**【问题 4】**

本问题主要考查网络流量控制技术。

网络畅通是网络建设中的基本要求，但是并非所有的网络流量都应该被转发，为了安全也为了满足部分业务流量的优先服务要求，总有一些流量需要被限制。常用的网络流量控制技术有访问控制列表（ACL）和服务质量（QoS）。QoS 主要有三种工作模式，一是 Best-Effort service（尽力而为的服务模型），是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大的可能性来发送报文。但对延时、可靠性等性能不提供任何保证。Best-Effort 服务模型是网络的缺省服务模型，通过 FIFO（first in first out 先入先出）队列来实现。它适用于绝大多数网络应用，如 FTP、E-Mail 等。二是 Integrated service（综合服务模型），它可以满足多种 QoS 需求。该模型使用资源预留协议（RSVP），RSVP 运行在从源端到目的端的每个设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。但是 Inter-Serv 模型对设备的要求很高，当网络中的数

据流数量很大时，设备的存储和处理能力会遇到很大的压力。Inter-Serv 模型可扩展性很差，难以在 Internet 核心网络实施。三是 Differentiated service（区分服务模型），Diff-Serv 是一个多服务模型，它可以满足不同的 QoS 需求。与 Int-Serv 不同，它不需要通知网络为每个业务预留资源，区分服务实现简单，扩展性较好，使用较为普遍。

**参考答案**

**【问题 1】**

（1）NAT 或网络地址转换

（2）ACL 或访问控制列表

（3）静态

（4）动态

**【问题 2】**

（5）deny

（6）permit ip any any

（7）61.192.93.100 61.192.93.102

（8）202.102.100.100 202.102.100.102

（9）list 101 pool ISP-B overload

（10）192.168.1.100 80 61.192.93.100 80

（11）192.168.1.100 80 202.102.100.100 80

**【问题 3】**

（12）ip nat outside

（13）ip nat outside

（14）ip nat inside

（15）ip route 61.192.93.0 255.255.255.0 s0

（16）ip route 0.0.0.0 0.0.0.0 s1

（17）配置备份路由，或者配置浮动静态路由

**【问题 4】**

（18）Best-Effort service 或尽力而为服务

（19）Differentiated service 或区分服务

（20）区分服务或 Differentiated service

**试题四（共 15 分）**

阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司网络拓扑结构如图 4-1 所示。公司内部使用 C 类私有 IP 地址，其中公司两个部门分别处于 VLAN10 和 VLAN20，VLAN10 采用 192.168.10.0/24 网段，VLAN20 采用

192.168.20.0/24 网段，每段最后一个地址作为网关地址。

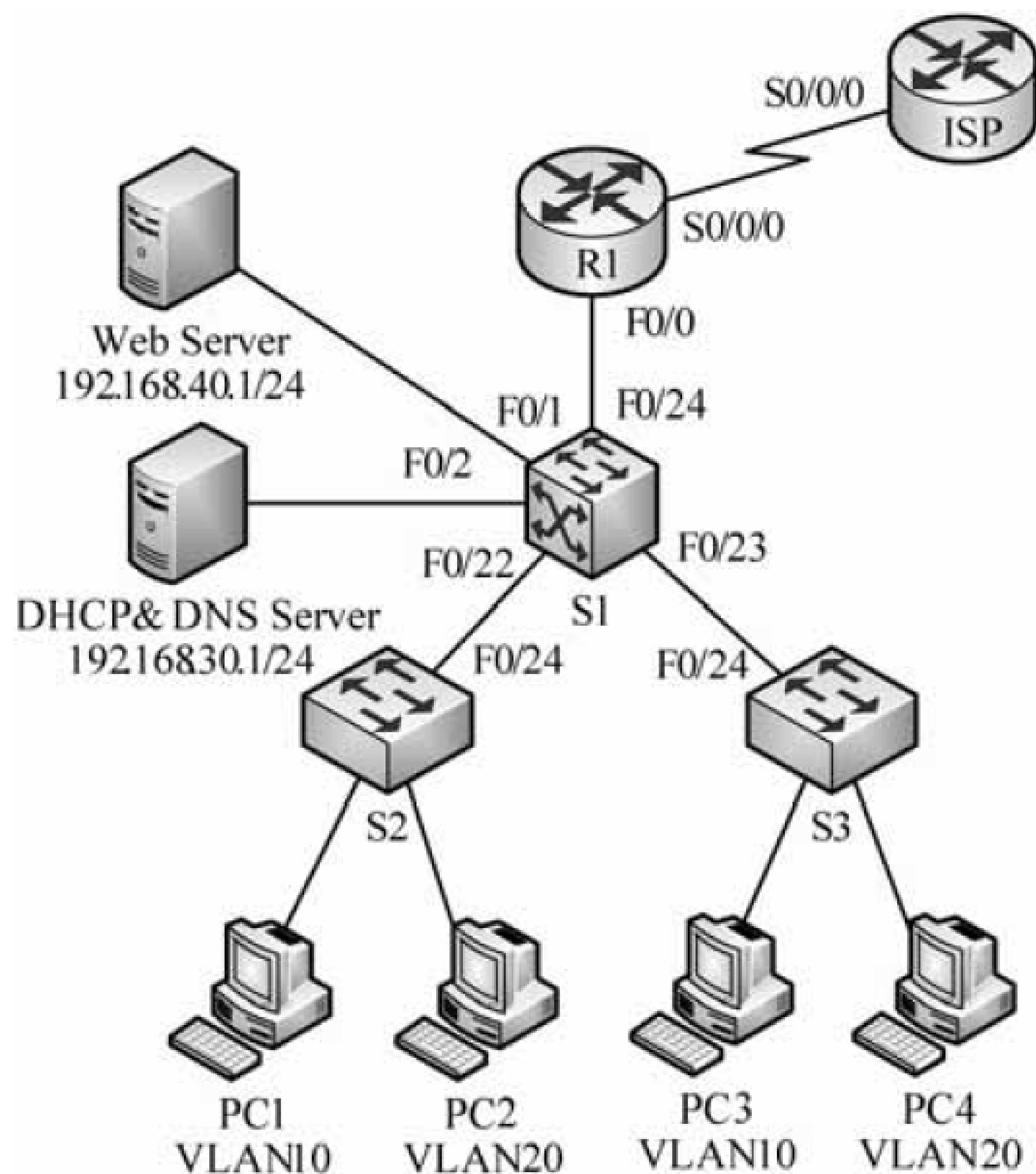



图 4-1

**【问题 1】（10 分）**

公司使用 VTP 协议规划 VLAN，三层交换机 S1 为 VTP Server，其他交换机为 VTP Client，并通过 S1 实现 VLAN 间通信。请根据网络拓扑和需求说明，完成交换机 S1 和 S2 的配置。

```
S1>enable
S1#configure terminal
S1(config)#vtp mode ____(1)____
S1(config)#vtp domain shx
S1(config)#vtp password shx
S1(config)#vlan 10
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#exit
S1(config)#interface vlan 10
S1(config-if)#ip address ____(2)____ ____(3)____
S1(config-vlan)#exit
S1(config)#interface vlan 20
S1(config-if)#ip address 192.168.20.254 255.255.255.0
S1(config-if)#exit
```

```
S1(config)#interface ___(4)___ fastethernet 0/22-23
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport mode ___(5)___
S1(config-if-range)#exit
S1(config)#interface fastEthernet 0/1
S1(config-if)#___(6)___                    //关闭二层功能
S1(config-if)#ip add 192.168.40.254 255.255.255.0
S1(config-if)#exit
……
S1(config)#___(7)___ ___(8)___             //开启路由功能
S1(config)#

S2>enable
S2#configure terminal
S2(config)#vtp mode ___(9)___
S2(config)#vtp domain shx
S2(config)#vtp password shx
S2(config)#interface fastethernet 0/24
S2(config-if)#switchport mode ___(10)___   //设定接口模式
S2(config-if)#end
S2#
```

**【问题 2】（5 分）**

公司申请了 202.165.200.0/29 地址段，使用 NAT-PT 为用户提供 Internet 访问，外部全局地址为 202.165.200.1，Web 服务器使用的外部映射地址为 202.165.200.3。请根据网络拓扑和需求说明，完成路由器 R1 的配置。

```
R1>enable
R1#config terminal
R1(config)#access-list 1 ___(11)___192.168.10.0 255.255.255.0
……
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 202.165.200.1 255.255.255.248
R1(config-if)#no shutdown
R1(config-if)#clock rate 4000000
R1(config-if)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.50.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip nat inside source___(12)___ 1 interface s0/0/0 overload
……
```

```
R1(config)#ip nat inside source static ___(13)___ 202.165.200.3
R1(config)#interface fastethernet 0/0
R1(config-if)#ip nat ___(14)___
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip nat ___(15)___
R1(config-if)#end
R1#
```

**试题四解析**

本题考查交换机和路由器的基本配置。

根据题目的需求，使用交换机 S1 作为 VTP Server，规划整个网络的 VLAN 配置，同时使用三层交换机 S1 实现两个 VLAN 之间的通信，需在 S1 上创建 SVI 接口，并配置 IP 地址，关闭交换机的二层功能。

在 R1 上使用 NAT-PT 实现局域网的 Internet 访问，将连接内部局域网的接口设置内部接口并指定转换的外部接口 IP 地址，同时将连接 Internet 的接口设置为外部接口。

**参考答案**

**【问题 1】**

（1）server

（2）192.168.10.254

（3）255.255.255.0

（4）range

（5）trunk

（6）no switchport

（7）ip

（8）routing

（9）client

（10）trunk

**【问题 2】**

（11）permit

（12）list

（13）192.168.40.1

（14）inside

（15）outside

# 第 25 章　2015 上半年网络工程师上午试题分析与解答

**试题（1）**

机器字长为 $n$ 位的二进制数可以用补码来表示 <u>（1）</u> 个不同的有符号定点小数。

（1）A．$2^n$　　B．$2^{n-1}$　　C．$2^n-1$　　D．$2^{n-1}+1$

**试题（1）分析**

本题考查计算机系统基础知识。

二进制数据在计算机系统中的表示方法是最基本的专业知识。补码本身是带符号位的，补码表示的数字中 0 是唯一的，不像原码有 +0 和–0 之分，也就意味着 $n$ 位二进制编码可以表示 $2^n$ 个不同的数。

**参考答案**

（1）A

**试题（2）**

计算机中 CPU 对其访问速度最快的是 <u>（2）</u> 。

（2）A．内存　　B．Cache　　C．通用寄存器　　D．硬盘

**试题（2）分析**

本题考查计算机系统基础知识。

计算机系统中的 CPU 内部对通用寄存器的存取操作是速度最快的，其次是 Cache，内存的存取速度再次，选项中访问速度最慢的就是作为外存的硬盘。它们共同组成分级存储体系来解决存储容量、成本和速度之间的矛盾。

**参考答案**

（2）C

**试题（3）**

计算机中 CPU 的中断响应时间指的是 <u>（3）</u> 的时间。

（3）A．从发出中断请求到中断处理结束

B．从中断处理开始到中断处理结束

C．CPU 分析判断中断请求

D．从发出中断请求到开始进入中断处理程序

**试题（3）分析**

本题考查计算机组成基础知识。

中断系统是计算机实现中断功能的软硬件总称。一般在 CPU 中设置中断机构，在外设接口中设置中断控制器，在软件上设置相应的中断服务程序。中断源在需要得到 CPU 服务时，请求 CPU 暂停现行工作转向为中断源服务，服务完成后，再让 CPU 回到原工作状态继续完成被打断的工作。中断的发生起始于中断源发出中断请求，中断处理过程中，中断系统需要解决一系列问题，包括中断响应的条件和时机，断点信息的保护与恢复，中断服务程序入口、中断处理等。中断响应时间，是指从发出中断请求到开始进入中断服务程序所需的时间。

**参考答案**

（3）D

**试题（4）**

总线宽度为 32bit，时钟频率为 200MHz，若总线上每 5 个时钟周期传送一个 32bit 的字，则该总线的带宽为__（4）__Mb/s。

（4）A．40　　B．80　　C．160　　D．200

**试题（4）分析**

本题考查计算机系统基础知识。

总线宽度是指总线的线数，即数据信号的并行传输能力，也体现总线占用的物理空间和成本；总线的带宽是指总线的最大数据传输率，即每秒传输的数据总量。总线宽度与时钟频率共同决定了总线的带宽。

$$32\text{bit} / 8 = 4\ \text{Byte}，\ 200\text{MHz} / 5 \times 4\ \text{Byte} = 160\ \text{Mb/s}$$

**参考答案**

（4）C

**试题（5）**

以下关于指令流水线性能度量的叙述中，错误的是__（5）__。

（5）A．最大吞吐率取决于流水线中最慢一段所需的时间

B．如果流水线出现断流，加速比会明显下降

C．要使加速比和效率最大化应该对流水线各级采用相同的运行时间

D．流水线采用异步控制会明显提高其性能

**试题（5）分析**

本题考查计算机系统结构的基础知识。

对指令流水线性能的度量主要有吞吐率，加速比和效率等指标。吞吐率是指单位时间内流水线所完成的任务数或输出结果的数量，最大吞吐率则是流水线在达到稳定状态后所得到的吞吐率，它取决于流水线中最慢一段所需的时间，所以该段成为流水线的瓶颈。流水线的加速比定义为等功能的非流水线执行时间与流水线执行时间之比，加速比

与吞吐率成正比，如果流水线断流，实际吞吐率将会明显下降，则加速比也会明显下降。流水线的效率是指流水线的设备利用率，从时空图上看效率就是 n 个任务所占的时空区与 m 个段总的时空区之比。因此要使加速比和效率最大化应该对流水线各级采用相同的运行时间。另外，流水线采用异步控制并不会给流水线性能带来改善，反而会增加控制电路的复杂性。

**参考答案**

（5）D

**试题（6）**

对高级语言源程序进行编译或解释的过程可以分为多个阶段，解释方式不包含__（6）__阶段。

（6）A. 词法分析　　B. 语法分析　　C. 语义分析　　D. 目标代码生成

**试题（6）分析**

本题考查程序语言基础知识。

用某种高级语言或汇编语言编写的程序称为源程序不能直接在计算机上执行。汇编语言源程序需要用一个汇编程序将其翻译成目标程序后才能执行。高级语言源程序则需要对应的解释程序或编译程序对其进行翻译，然后在机器上运行。

解释程序也称为解释器，它或者直接解释执行源程序，或者将源程序翻译成某种中间代码后再加以执行；而编译程序（编译器）则是将源程序翻译成目标语言程序，然后在计算机上运行目标程序。这两种语言处理程序的根本区别是：在编译方式下，机器上运行的是与源程序等价的目标程序，源程序和编译程序都不再参与目标程序的执行过程；而在解释方式下，解释程序和源程序（或其某种等价表示）要参与到程序的运行过程中，运行程序的控制权在解释程序。简单来说，在解释方式下，翻译源程序时不生成独立的目标程序，而编译器则将源程序翻译成独立保存的目标程序。

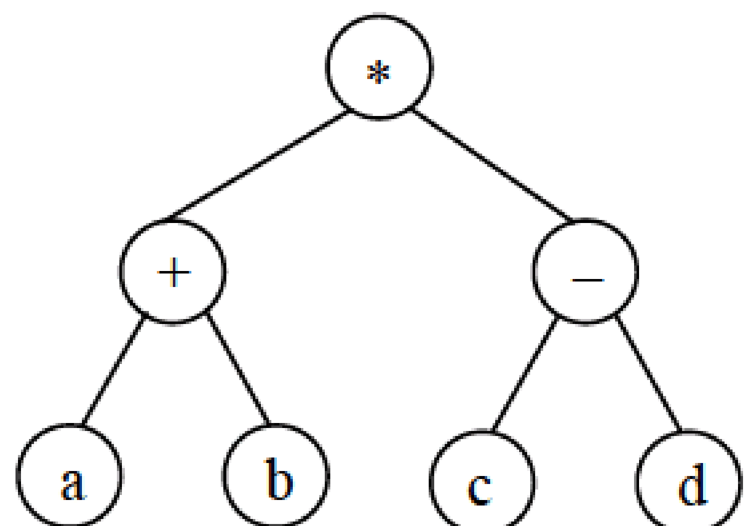
**参考答案**

（6）D

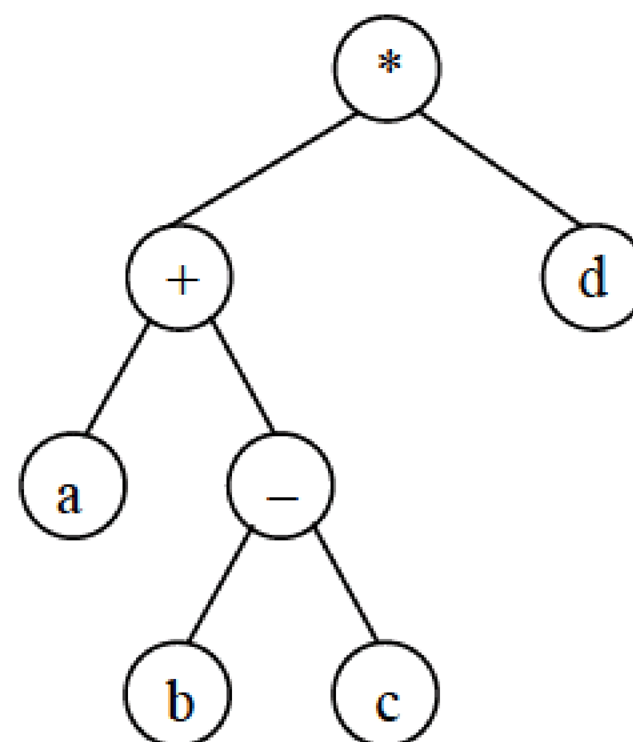
**试题（7）**

与算术表达式“(a+(b−c))*d”对应的树是__（7）__。

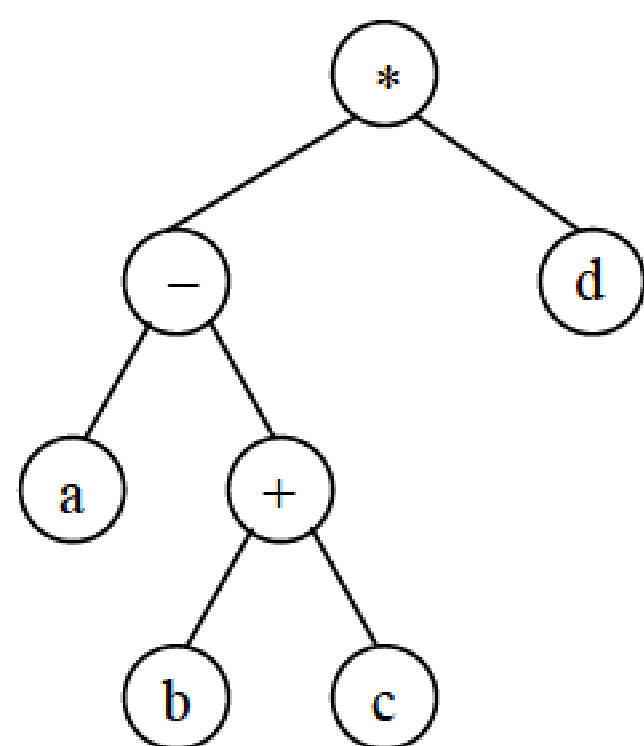
（7）A.



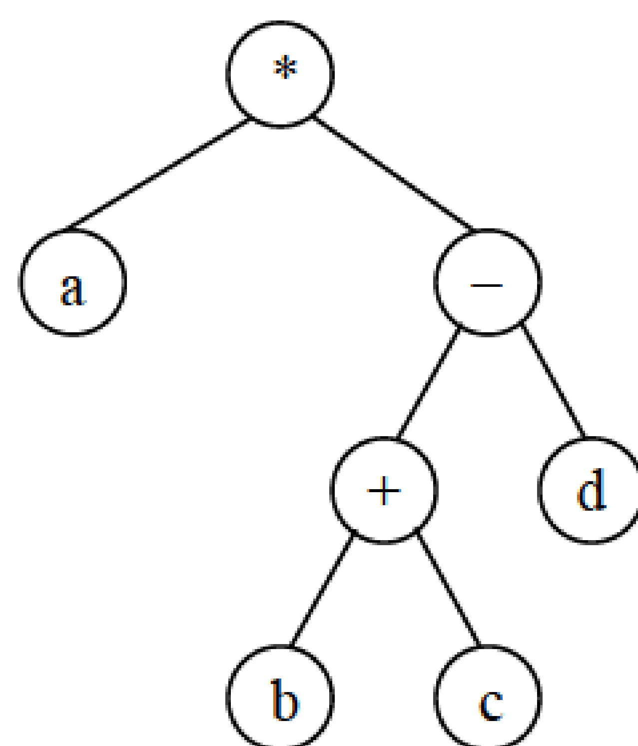

B.



C.




D.




**试题（7）分析**

本题考查程序语言与数据结构基础知识。

对算术表达式“(a+(b–c))*d”求值的运算处理顺序是：先进行 b–c，然后与 a 相加，最后再与 d 相乘。只有选项 B 所示的二叉树与其相符。

**参考答案**

（7）B

**试题（8）**

C 程序中全局变量的存储空间在＿（8）＿分配。

（8）A. 代码区　B. 静态数据区　C. 栈区　D. 堆区

**试题（8）分析**

本题考查程序语言基础知识。

程序运行时的用户内存空间一半划分为代码区、静态数据区、栈区和堆区，其中栈区和堆区也称为动态数据区。全局变量的存储空间在静态数据区。

**参考答案**

（8）B

**试题（9）**

某进程有 4 个页面，页号为 0～3，页面变换表及状态位、访问位和修改位的含义如下图所示。系统给该进程分配了 3 个存储块，当采用第二次机会页面替换算法时，若访问的页面 1 不在内存，这时应该淘汰的页号为＿（9）＿。

| 页号 | 页帧号 | 状态位 | 访问位 | 修改位 |
|---|---|---|---|---|
| 0 | 6 | 1 | 1 | 1 |
| 1 | — | 0 | 0 | 0 |
| 2 | 3 | 1 | 1 | 1 |
| 3 | 2 | 1 | 1 | 0 |

状态位含义 {=0 不在内存; =1 在内存}

访问位含义 {=0 未访问过; =1 访问过}

修改位含义 {=0 未修改过; =1 修改过}

（9）A. 0　B. 1　C. 2　D. 3

**试题（9）分析**

试题（9）的正确选项为 D。根据题意页面变换表中状态位等于 0 和 1 分别表示页面不在内存或在内存，所以 0、2 和 3 号页面在内存。当访问的页面 1 不在内存时，系统应该首先淘汰未被访问的页面，因为根据程序的局部性原理最近未被访问的页面下次被访问的概率更小；如果页面最近都被访问过，应该先淘汰未修改过的页面。因为未修改过的页面内存与辅存一致，故淘汰时无须写回辅存，使系统页面置换代价小。经上述分析，0、2 和 3 号页面都是最近被访问过的，但 0 和 2 号页面都被修改过而 3 号页面未修改过，故应该淘汰 3 号页面。

**参考答案**

（9）D

**试题（10）**

王某是某公司的软件设计师，每当软件开发完成后均按公司规定编写软件文档，并提交公司存档。那么该软件文档的著作权__（10）__享有。

（10）A．应由公司

B．应由公司和王某共同

C．应由王某

D．除署名权以外，著作权的其他权利由王某

**试题（10）分析**

本题考查知识产权的基本知识。

依据著作权法第十一条、第十六条规定，职工为完成所在单位的工作任务而创作的作品属于职务作品。职务作品的著作权归属分为两种情况。

① 虽是为完成工作任务而为，但非经法人或其他组织主持，不代表其意志创作，也不由其承担责任的职务作品，如教师编写的教材，著作权应由作者享有，但法人或者其他组织有权在其业务范围内优先使用的权利，期限为 2 年。

② 由法人或者其他组织主持，代表法人或者其他组织意志创作，并由法人或者其他组织承担责任的职务作品，如工程设计、产品设计图纸及其说明、计算机软件、地图等职务作品，以及法律规定或合同约定著作权由法人或非法人单位单独享有的职务作品，作者享有署名权，其他权利由法人或者其他组织享有。

**参考答案**

（10）A

**试题（11）**

当登录交换机时，符号__（11）__是特权模式提示符。

（11）A．@　　B．#　　C．>　　D．&

**试题（11）分析**

登录交换机时首先遇到的符号是>，这表示交换机处于用户执行模式。

```
Switch>
```

这时输入 enable 命令，则交换机进入特权模式

```
Switch >enable
Switch#
```

进入全局配置模式的命令是 Switch#config terminal

```
Switch(config)# （配置模式提示符）
```

**参考答案**

（11）B

**试题（12）**

下面的选项中显示系统硬件和软件版本信息的命令是＿（12）＿。

（12）A．show configuration　　B．show environment

C．show version　　D．show platform

**试题（12）分析**

路由器显示命令如下所示：

| | |
|---|---|
| 查看版本及引导信息 | show version |
| 查看运行设置 | show running-config |
| 查看开机设置 | show startup-config |
| 显示端口信息 | show interface *type slot/number* |
| 显示路由信息 | show ip route |

**参考答案**

（12）C

**试题（13）**

Cisco 路由器高速同步串口默认的封装协议是＿（13）＿。

（13）A．PPP　　B．LAPB　　C．HDLC　　D．ATM-DXI

**试题（13）分析**

路由器不仅能实现局域网之间的连接，还能实现局域网与广域网、广域网与广域网之间的连接。路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 口。常见的网络端口有以下几种：

① RJ-45 端口：这种端口通过双绞线连接以太网。可实现 10M/100M/1000M 高速数

据传输。

② 高速同步串口：路由器通过高速同步串口（Synchronous Serial Port）连接 DDN、帧中继、X.25 等网络。高速同步串口默认的封装协议是 HDLC。

③ 异步串口：异步串口（ASYNC）主要用于与 Modem 的连接，以实现远程计算机通过 PSTN 拨号接入。

④ Console 端口：Console 端口通过专用电缆连接至计算机串行口，利用终端仿真程序对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。

⑤ AUX 端口：这是用于远程配置的异步端口（Auxiliary Prot），主要用于拔号连接，还可通过收发器连接 MODEM，支持硬件流控。

⑥ SC 端口：这是光纤端口，用于连接到具有光纤端口的交换机，一般以“100b FX”标注，传输距离可以达到几百米甚至几千米，传输速率能够达到 1Gb/s 或 10Gb/s。另外还有 GBIC 插槽和 SFP 插槽，SFP 比 GBIC 占用的位置少，可以适应各种复杂的网络环境。

**参考答案**

（13）C

**试题（14）**

以下关于网桥和交换机的区别的叙述中，正确的是__（14）__。

（14）A．交换机主要是基于软件实现，而网桥是基于硬件实现的
　　B．交换机定义了广播域，而网桥定义了冲突域
　　C．交换机根据 IP 地址转发，而网桥根据 MAC 地址转发
　　D．交换机比网桥的端口多，转发速度更快

**试题（14）分析**

传统的网桥是在计算机上安装两个网卡，通过网桥软件实现局域网之间的帧转发，而交换机则是基于硬件实现的高速转发设备，标准的商用交换机都具有 24 个端口。

**参考答案**

（14）D

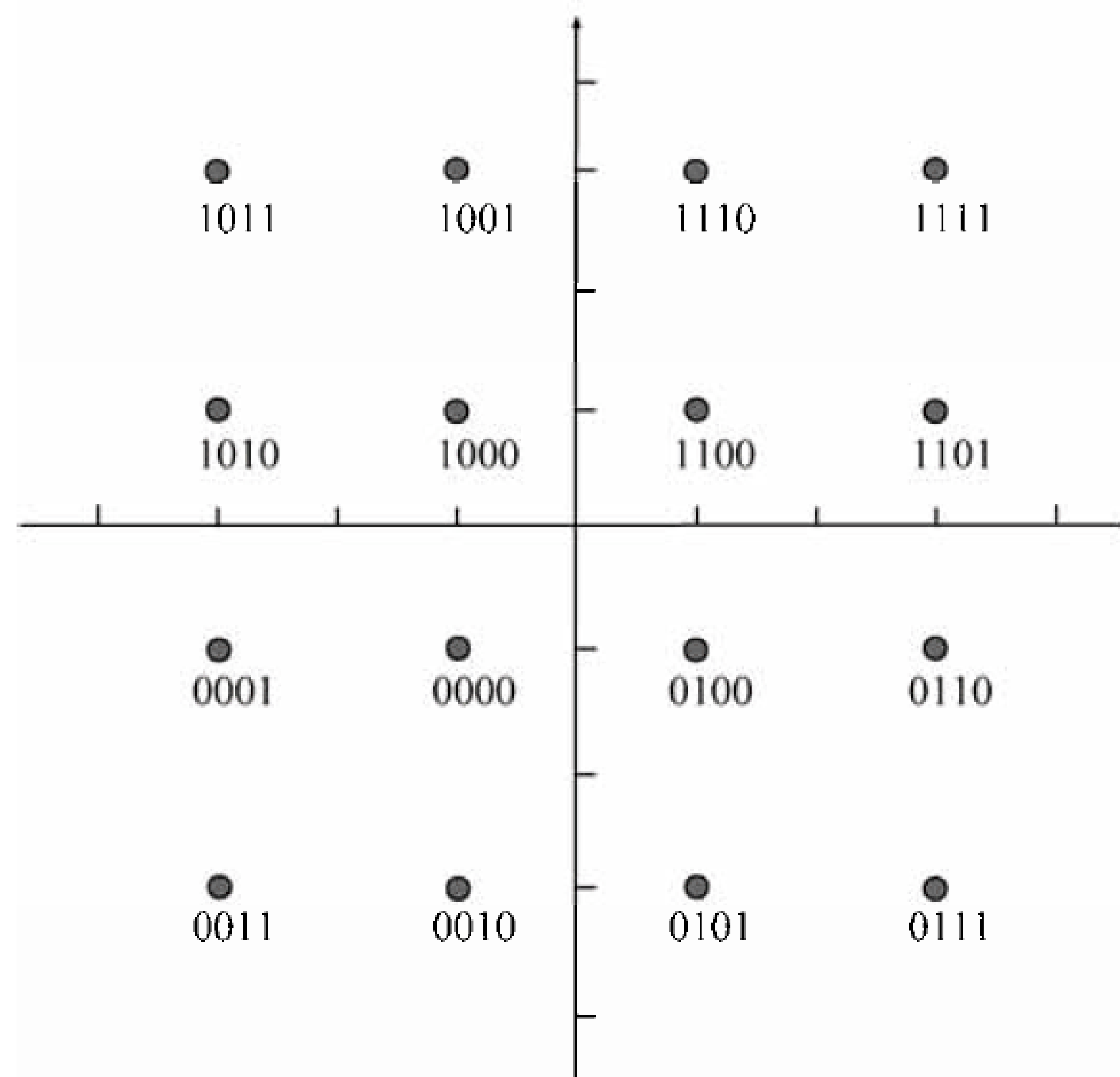
**试题（15）**

正交幅度调制 16-QAM 的数据速率是码元速率的__（15）__倍。

（15）A．2　　B．4　　C．8　　D．16

**试题（15）分析**

正交幅度调制（Quadrature Amplitude Modulation，QAM）是把两个幅度相同但相位相差 90° 的模拟信号合成为一个载波信号，经过信道编码后把数据组合映射到星座图上，如下图所示。




QAM 调制实际上是幅度调制和相位调制的组合，同时利用了载波的幅度和相位来传递数据信息。与单纯的 PSK 调制相比，在最小距离相同的条件下，QAM 星座图中可以容纳更多的载波码点，可以实现更高的频带利用率。16-QAM 是用一个码元表示 4 比特二进制数据，它的数据速率是码元速率的 4 倍。目前最高可以达到 1024-QAM，即用一个码元表示 10 比特数据。

**参考答案**

（15）B

**试题（16）**

电话线路使用的带通滤波器的带宽为 3kHz（300～3300Hz），根据奈奎斯特采样定理，最小采样频率应为 （16） 。

（16）A. 300 Hz　　B. 3300 Hz　　C. 6000 Hz　　D. 6600 Hz

**试题（16）分析**

PCM 主要经过 3 个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组。

采样的频率决定了可恢复的模拟信号的质量。根据奈奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即 $f=1/T=2f_{max}$，其中，$f$ 为采样频率，$T$ 为采样周期，$f_{max}$ 为信号的最高频率。

人耳对 25～22 000 Hz 的声音有反应。在谈话时，大部分有用的信息的能量分布在 200 Hz～3500 Hz 之间。因此，电话线路使用的带通滤波器的带宽为 3 kHz（即 300～3300Hz）。根据 Nyquist 采样定理，最小采样频率应为 6600 Hz，实际上，CCITT 规定对

话音信号的采样频率为 8kHz。

**参考答案**

（16）D

**试题（17）**

当一个帧离开路由器接口时，其第二层封装信息中__（17）__。

（17）A. 数据速率由 10Base-TX 变为 100Base-TX

B. 源和目标 IP 地址改变

C. 源和目标 MAC 地址改变

D. 模拟线路变为数字线路

**试题（17）分析**

帧头中的主要信息是源和目标的 MAC 地址，另外还有一些用于帧控制的信息。数据速率和调制方式（模拟/数字）属于物理层机制，而 IP 地址则属于网络层信息，都与第二层封装信息无关。

**参考答案**

（17）C

**试题（18）**

__（18）__时使用默认路由。

（18）A. 访问本地 Web 服务器　　B. 在路由表中找不到目标网络

C. 没有动态路由　　D. 访问 ISP 网关

**试题（18）分析**

在路由表中找不到目标网络时使用默认路由。默认路由通常指本地网关的地址。

**参考答案**

（18）B

**试题（19）**

以下关于 OSPF 的区域（Area）的叙述中，正确的是__（19）__。

（19）A. 各个 OSPF 区域都要连接到主干区域

B. 分层的 OSPF 网络不需要多个区域

C. 单个 OSPF 网络只有区域 1

D. 区域 ID 的取值范围是 1～32768

**试题（19）分析**

为了适应大型网络配置的需要，OSPF 协议引入了“分层路由”的概念。如果网络规模很大，则路由器要学习的路由信息很多，对网络资源的消耗很大，所以典型的链路状态协议都把网络划分成较小的区域（Area），从而限制了路由信息传播的范围。每个区域就如同一个独立的网络，区域内的路由器只保存该区域的链路状态信息，使得路由器的链路状态数据库可以保持合理的大小，路由计算的时间和报文数量都不会太大。OSPF

主干网负责在各个区域之间传播路由信息。

每个 OSPF 区域被指定了一个 32 位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为 0.0.0.0（Area 0），各个 OSPF 区域都要连接到主干区域。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

- 标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。
- 主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。
- 存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。
- 完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。
- 不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（19）A

**试题（20）**

运行 OSPF 协议的路由器用__（20）__报文来建立和更新它的拓扑数据库。

（20）A. 由其他路由器发送的链路状态公告（LSA）

B. 从点对点链路收到的信标

C. 由指定路由器收到的 TTL 分组

D. 从邻居路由器收到的路由表

**试题（20）分析**

OSPF 路由器之间通过链路状态公告（Link State Advertisement，LSA）交换网络拓扑信息，建立和更新自己的拓扑数据库。LSA 中包含连接的接口、链路的度量值（Metric）等信息。

**参考答案**

（20）A

**试题（21）**

链路状态路由协议的主要特点是__（21）__。

（21）A. 邻居之间交换路由表　　B. 通过事件触发及时更新路由

C. 周期性更新全部路由表　　D. 无法显示整个网络拓扑结构

**试题（21）分析**

运行链路状态路由协议（例如 OSFP）的路由器通过各自的接口连接到一个共同的

网络上，它们之间是邻居关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器（DR），其他路由器都与 DR 建立毗邻关系，把自己掌握的链路状态信息提交给 DR，由 DR 代表这个网络向外界发布，所以链路状态协议是通过组播机制来共享路由信息的。链路状态协议只是在网络拓扑结构出现变化时才通过事件触发机制增量式地发送路由更新消息。与之相反，距离矢量协议是在邻居之间周期性地交换路由表。

**参考答案**

（21）B

**试题（22）**

从下面一条 RIP 路由信息中可以得到的结论是__（22）__。

| **R 10.10.10.7 [120/2] via 10.10.10.8,00:00:24,Serial 0/1** |
|---|

（22）A．下一个路由更新将在 36 秒之后到达
　　B．到达目标 10.10.10.7 的距离是两跳
　　C．串口 S0/1 的 IP 地址是 10.10.10.8
　　D．串口 S0/1 的 IP 地址是 10.10.10.7

**试题（22）分析**

这一条 RIP 路由信息说明到达目标 10.10.10.7 的距离是两跳，下一跳的地址是 10.10.10.8，通过本地串口 S0/1 转发。

**参考答案**

（22）B

**试题（23）**

运行距离矢量路由协议的路由器__（23）__。

（23）A．把路由表发送到整个路由域中的所有路由器
　　B．使用最短通路算法确定最佳路由
　　C．根据邻居发来的信息更新自己的路由表
　　D．维护整个网络的拓扑数据库

**试题（23）分析**

运行距离矢量路由协议的路由器把自己的路由表发送给邻居路由器，邻居路由器根据收到的路由信息更新自己的路由表，再向其他邻居发送自己的路由表。这样使得路由变化信息在整个网络中逐步扩散开来。每个路由器只知道它连接的邻居，而不能了解整个网络的拓扑连接情况。

**参考答案**

（23）C

**试题（24）**

以下关于 VLAN 的叙述中，正确的是__（24）__。

（24）A．VLAN 对分组进行过滤，增强了网络的安全性

B．VLAN 提供了在大型网络中保护 IP 地址的方法

C．VLAN 在可路由的网络中提供了低延迟的互联手段

D．VLAN 简化了在网络中增加、移除和移动主机的操作

**试题（24）分析**

把局域网划分成多个不同的 VLAN，使得网络接入不再局限于物理位置的约束，这样就简化了在网络中增加、移除和移动主机的操作，特别是动态配置的 VLAN，无论主机插在哪里，它都处于自己的 VLAN 中。VLAN 内部可以相互通信，VLAN 之间不能直接通信，必须经过特殊设置的路由器才可以连通。这样做的结果是，通过在较大的局域网中创建不同的 VLAN，可以抵御广播风暴的影响，也可以通过设置防火墙来提高网络的安全性。VLAN 并不能直接增强网络的安全性。

**参考答案**

（24）D

**试题（25）**

当局域网中更换交换机时，怎样保证新交换机成为网络中的根交换机？ （25） 

（25）A．降低网桥优先级

B．改变交换机的 MAC 地址

C．降低交换机端口的根通路费用

D．为交换机指定特定的 IP 地址

**试题（25）分析**

在交换式局域网中由环路引起的循环转发破坏了网桥的数据库，使得网桥无法获得正确的转发信息。为了消除环路，从而发明了生成树协议。该协议规定，生成树的根是通过分布式选举算法产生的。每一个网桥有唯一的优先级和唯一的 MAC 地址，优先级+MAC 地址构成网桥的标识符，标识符最小的网桥自动成为生成树的根桥。所以要保证新交换机成为网络中的根交换机，则必须降低网桥优先级。

**参考答案**

（25）A

**试题（26）**

双绞线电缆配置如下图所示，这种配置支持 （26） 之间的连接。

| Pin Number | Color | Function | Pin | Color | Function |
|---|---|---|---|---|---|
| 1 | white/Green | TX+ | 3 | Orange | RX+ |
| 2 | Green | TX– | 6 | white/Orange | RX– |
| 3 | white/Orange | RX+ | 1 | Green | TX+ |
| 6 | Orange | RX– | 2 | white/Green | TX– |

（26）A．PC 到路由器　　　　B．PC 到交换机
　　　C．服务器到交换机　　D．交换机到路由器

**试题（26）分析**

图中的双绞线是交叉双绞线，用来连接同类设备，4 个选项中只有 PC 和路由器是同类设备。

**参考答案**

（26）A

**试题（27）**

参见下图的网络配置，发现工作站 B 无法与服务器 A 通信，什么故障影响了两者互通？__（27）__

Server A
IP:131.1.123.24/27
GW:131.1.123.33

Workstation B
IP:131.1.123.43/27
GW:131.1.123.33

（27）A．服务器 A 的 IP 地址是广播地址
　　　B．工作站 B 的 IP 地址是网络地址
　　　C．工作站 B 与网关不属于同一子网
　　　D．服务器 A 与网关不属于同一子网

**试题（27）分析**

服务器 A 的 IP 地址 131.1.123.24/27：**10000011.00000001. 01111011.000**11000 服务器 A 的地址不是广播地址。

服务器 A 的网关地址 131.1.123.33：**10000011.00000001. 01111011.001**00001 这个地址与服务器 A 的地址不属于同一个子网。

工作站 B 的 IP 地址 131.1.123.43/27：**10000011.00000001. 01111011.001**01011 这个地址不是网络地址。

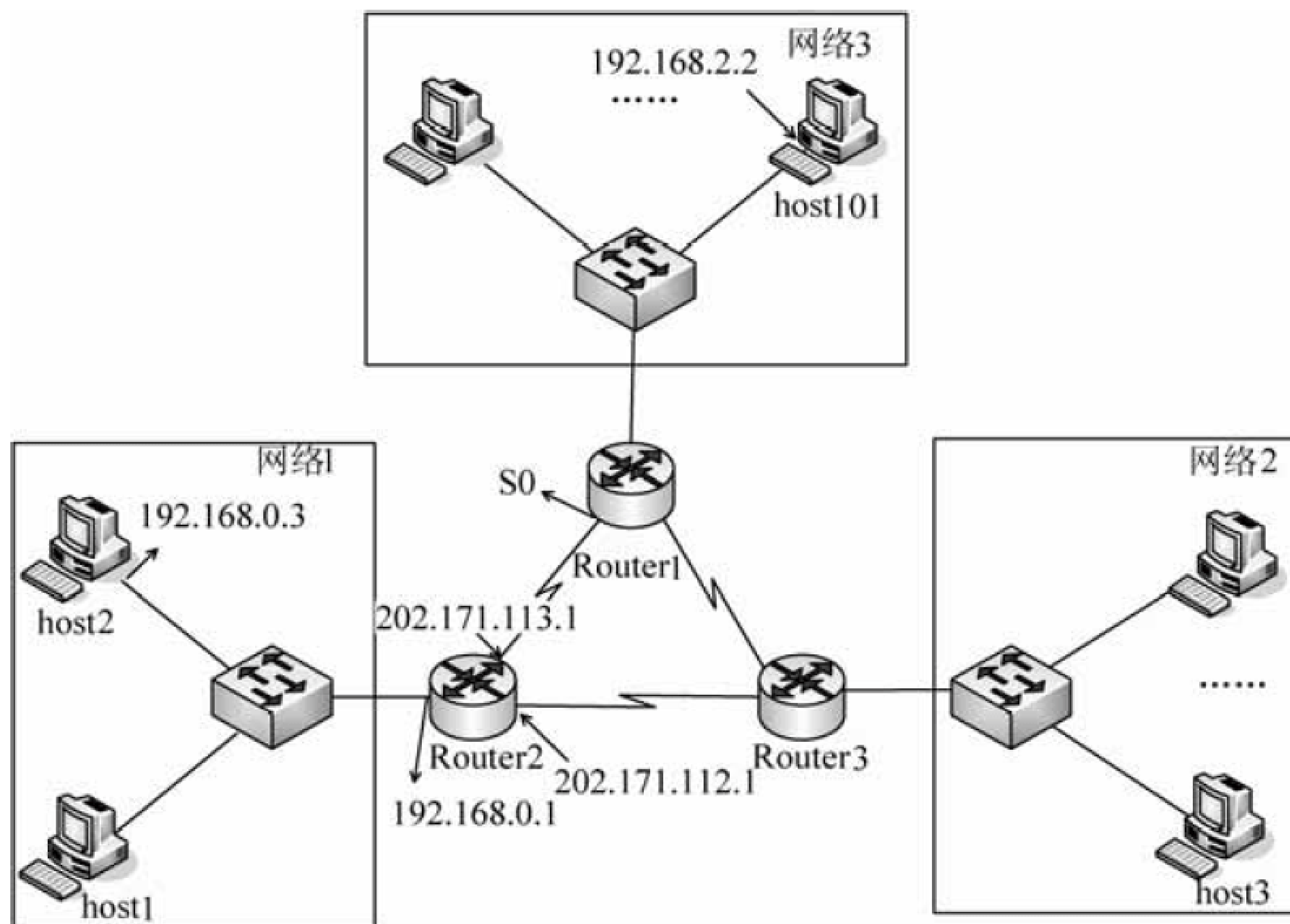
工作站 B 的网关地址 131.1.123.33：**10000011.00000001. 01111011.001**00001 工作站 B 与网关属于同一个子网。

**参考答案**

（27）D

**试题（28）**

某网络拓扑图如下所示，若采用 RIP 协议，在路由器 Router2 上需进行 RIP 声明的网络是__（28）__。




（28）A．仅网络 1

B．网络 1、202.117.112.0/30 和 202.117.113.0/30

C．网络 1、网络 2 和网络 3

D．仅 202.117.112.0/30 和 202.117.113.0/30

**试题（28）分析**

本题考查路由器上 RIP 路由协议的配置。

在路由器中采用 RIP 协议时，每个路由器需要声明直接连接的各个网络，路由器 Router2 直接连接了网络 1、202.117.112.0/30 和 202.117.113.0/30 三个网络，均需进行声明。

**参考答案**

（28）B

**试题（29）**

IIS 服务身份验证方式中，安全级别最低的是__（29）__。

（29）A．.NET Passport 身份验证　　B．集成 Windows 身份验证

C．基本身份验证　　D．摘要式身份验证

**试题（29）分析**

本题考查 IIS 服务器配置及安全性等知识。

IIS 服务身份验证方式有摘要式身份验证、基本身份验证、.NET Passport 身份验证

和集成 Windows 身份验证，其中安全级别最低的是基本身份验证。

**参考答案**

（29）C

**试题（30）**

有较高实时性要求的应用是__（30）__。

（30）A．电子邮件　B．网页浏览　C．VoIP　D．网络管理

**试题（30）分析**

本题考查 Internet 应用及相关知识。

不同的应用有不同的实时性要求，电话、音频和视频有较高的实时性要求。故有较高实时性要求的应用是 VoIP。

**参考答案**

（30）C

**试题（31）**

在 Linux 中，文件__（31）__用于解析主机域名。

（31）A．etc/hosts　B．etc/host.conf　C．etc/hostname　D．etc/bind

**试题（31）分析**

本题考查 Linux 系统文件的基本知识。

etc/hosts 中包含了 IP 地址和主机名之间的映射，还包括主机名的别名；etc/host.conf 文件指定如何解析主机域名，Linux 通过解析器库来获得主机名对应的 IP 地址；etc/hostname 文件中包含了 Linux 系统的主机名称，包括完全的域名；D 选项中的 etc/bind 是一个干扰项。

**参考答案**

（31）B

**试题（32）**

在 Linux 中，要删除用户组 group1 应使用__（32）__命令。

（32）A．[root@localhost]#delete group1

B．[root@localhost]#gdelete group1

C．[root@localhost]#groupdel group1

D．[root@localhost]#gd group1

**试题（32）分析**

本题考查 Linux 系统命令的使用方法。

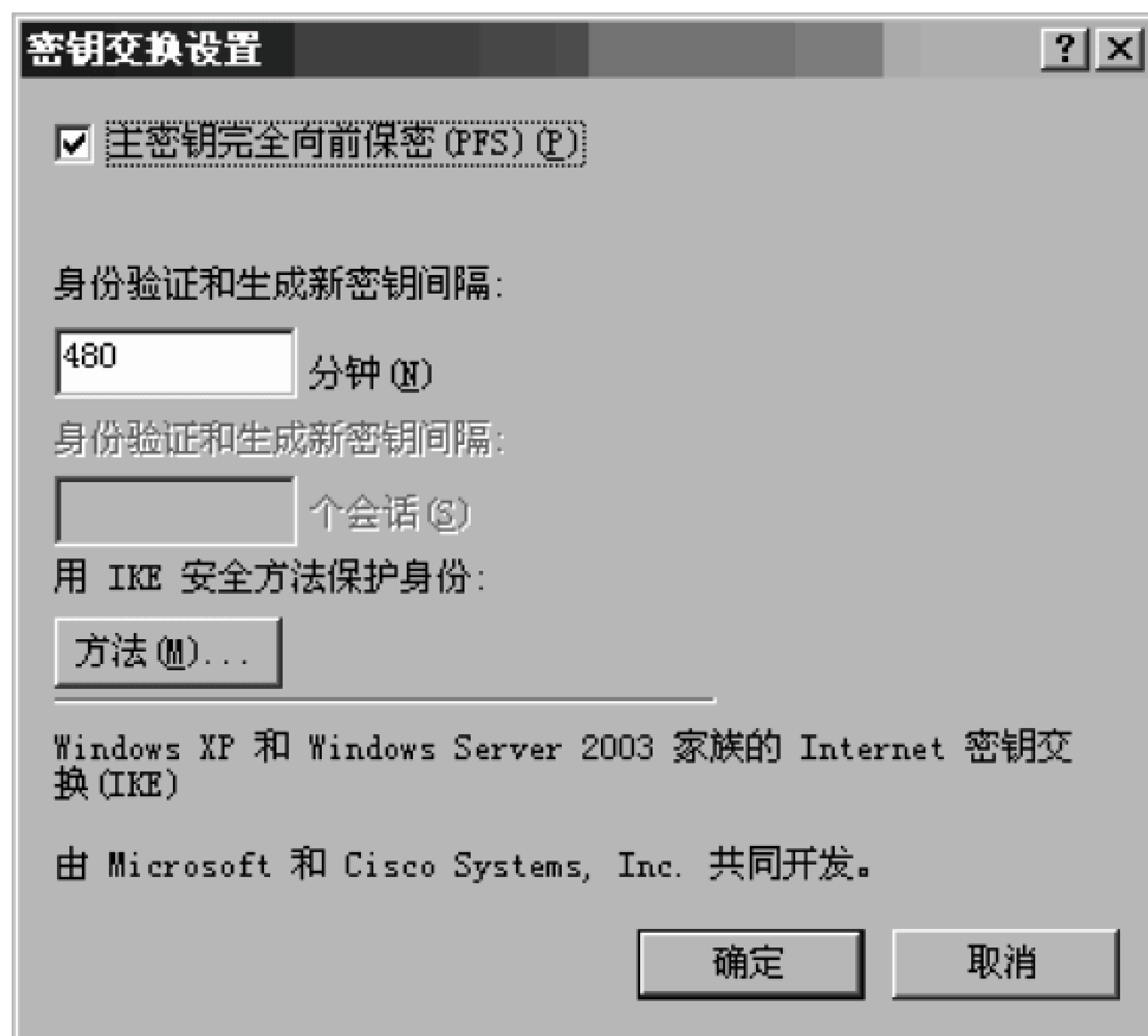
要删除用户组需使用的命令是 groupdel group1，其他各个选项均为错误的对命令的缩写和简写。

**参考答案**

（32）C

**试题（33）**

Windows Server 2003 采用 IPSec 进行保密通信，如果密钥交换采用“主密钥完全向前保密（PFS）”，则“身份验证和生成密钥间隔”默认值为 480 分钟和__（33）__个会话。




（33）A．1　　B．2　　C．161　　D．530

**试题（33）分析**

本题考查 IPSec 基础知识。

IPSec 使用称为动态重新加密的方法来控制通信过程中生成新密钥的频率。通信以块的形式发送，对每个数据块都使用不同的密钥进行保护。这样可防止已经获取部分通信和相应的会话密钥的攻击者获取其余部分的通信。如果“启用主密钥完全向前保密（PFS）”，则不使用快速模式会话密钥刷新限制。

将会话密钥刷新限制设置为 1，与启用主密钥 PFS 的效果相同。

**参考答案**

（33）A

**试题（34）**

在 Windows 用户管理中，使用组策略 A-G-DL-P，其中 P 表示__（34）__。

（34）A．用户账号　　B．资源访问权限
C．域本地组　　D．通用组

**试题（34）分析**

本题考查 Windows 用户管理的组策略基础知识。

组策略 A-G-DL-P 中 A 表示用户账号，G 表示全局组，DL 表示域本地组，P 表示资源访问权限（Permission）。A-G-DL-P 策略是将用户账号添加到全局组中，将全局组添加到另一个域的域本地组中，然后为域本地组分配本地资源的访问权限，这样来自其他

域的用户就可以访问本地域中的资源了。

**参考答案**

（34）B

**试题（35）**

以下叙述中，不属于无源光网络优势的是__（35）__。

（35）A．设备简单，安装维护费用低，投资相对较小

B．组网灵活，支持多种拓扑结构

C．安装方便，不要另外租用或建造机房

D．无源光网络适用于点对点通信

**试题（35）分析**

本题考查无源光网络（PON）方面的基础知识。

无源光网络（PON）是一种纯介质网络，避免了外部设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统可靠性，同时节省了维护成本。

分光器就是连接 OLT 和 ONU 的无源设备，它的功能是分发下行数据，并集中上行数据。分光器带有一个上行光接口，若干下行光接口，实现点对多点的通讯。

**参考答案**

（35）D

**试题（36）**

查看 DNS 缓存记录的命令是__（36）__。

（36）A．ipconfig /flushdns　　B．nslookup

C．ipconfig /release　　D．ipconfig /displaydns

**试题（36）分析**

本题考查 ipconfig 及 nslookup 网络管理命令。

ipconfig /flushdns 是清除 DNS 缓存记录；ipconfig /displaydns 为显示 DNS 缓存记录；nslookup 为显示域名解析服务器；ipconfig /release 是释放 DHCP 自动分配的 IP 地址。

**参考答案**

（36）D

**试题（37）**

在 Windows 操作系统中，__（37）__文件可以帮助域名解析。

（37）A．Cookie　　B．index

C．hosts　　D．default

**试题（37）分析**

本题考查 hosts 域名解析文件。

在 Windows 操作系统中，可以帮助域名解析的文件是 hosts。

**参考答案**

（37）C

**试题（38）**

DHCP__（38）__报文的目的 IP 地址为 255.255.255.255。

（38）A．DhcpDiscover　　B．DhcpOffer
　　C．DhcpNack　　D．DhcpAck

**试题（38）分析**

本题考查 DHCP 的报文格式。

四种报文格式中，采用广播的只有 DhcpDiscover。当主机启动时需要自动分配 IP 地址，又不知道 DHCP 服务器地址，故请求报文 DhcpDiscover 中目的 IP 地址为 255.255.255.255。

**参考答案**

（38）A

**试题（39）**

客户端采用__（39）__报文来拒绝 DHCP 服务器提供的 IP 地址。

（39）A．DhcpOffer　　B．DhcpDecline
　　C．DhcpAck　　D．DhcpNack

**试题（39）分析**

本题考查 DHCP 的报文格式及各自应用场合。

DhcpOffer 为 DHCP 服务器给客户机提供 IP 地址的相应报文；如果客户端拒绝服务器提供的 IP 地址，采用 DhcpDecline；当 DHCP 服务器接收到客户端的 Dhcprequest 之后，会向客户端发出一个 DHCPACK 回应提供地址给客户，或者发出一个 DHCPNACK 回应不提供地址给客户。

**参考答案**

（39）B

**试题（40）**

若一直得不到回应，DHCP 客户端总共会广播__（40）__次请求。

（40）A．3　　B．4　　C．5　　D．6

**试题（40）分析**

本题考查 DHCP 协议的工作模式。

在 Windows 的预设情形下，Dhcpdiscover 的等待时间预设为 1 秒，也就是当客户端将第一个 Dhcpdiscover 包送出去之后，在 1 秒之内没有得到回应的话，就会进行第二次 Dhcpdiscover 广播。若一直得不到回应的情况下，客户端一共会有 4 次 Dhcpdiscover 广播，除了第一次会等待 1 秒之外，其余三次的等待时间分别是 9，13，16 秒。如果都没有得到 DHCP 服务器的回应，客户端则会显示错误信息，宣告 Dhcpdiscover 的失败。

之后，基于使用者的选择，系统会继续在 5 分钟之后再重复一次 Dhcpdiscover 的过程。

**参考答案**

（40）B

**试题（41）**

提供电子邮件安全服务的协议是__（41）__。

（41）A．PGP　　B．SET　　C．SHTTP　　D．Kerberos

**试题（41）分析**

本题考查安全电子邮件协议的基础知识。

PGP（Pretty Good Privacy）是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。它能够在各种平台上免费试用，并得到了众多的制造商支持。PGP 提供数据加密和数字签名服务，可用于电子邮件的加密和签名。

SET（Secure Electronic Transaction）是安全电子交易的英文简写，它是一种安全协议和报文格式的集合，融合了 Netscape 的 SSL、Microsoft 的 STT、Terisa 的 S-HTTP 以及 PKI 技术，通过数字证书和数字签名机制，使得客户可以与供应商进行安全的电子交易。目前，SET 已经获得了 Mastercard、Visa 等众多厂商的支持，成为电子商务安全中的安全基础设施。

SHTTP 也可以写作 S-HPPT，是一种面向报文的安全通信协议，其目的是保证商业贸易信息的传输安全，促进电子商务的发展。但是在 SSL 出现后，S-HTTP 并未获得广泛的应用，目前，SSL 基本已经取代了 S-HTTP。

Kerberos 是一项认证服务，它要解决的问题是在公开的分布式环境中，工作站上的用户希望通过安全的方式访问分布在网络的服务器。

**参考答案**

（41）A

**试题（42）**

IDS 设备的主要作用是__（42）__。

（42）A．用户认证　　B．报文认证

C．入侵检测　　D．数据加密

**试题（42）分析**

本题考查的是网络安全设备的功能。

IDS（Intrusion Detection System）入侵检测系统，是作为防火墙之后的第二道安全屏障，通过从网络中关键地点收集信息并对其进行分析，从中发现违反安全策略的行为和遭到入侵攻击的迹象，并自动做出响应。

它的主要功能包括对用户和系统行为的监测与分析、系统安全漏洞的检查和扫描、重要文件的完整性评估、已知攻击行为的识别、异常行为模式的统计分析、操作系统的审计跟踪，以及违反安全策略的用户行为的检测等。入侵检测通过实时地监控入侵事件，

在造成系统损坏或数据丢失之前阻止入侵者进一步的行动，使系统能尽快恢复正常工作。同时还要收集有关入侵的技术资料，用于改进和增强系统抵抗入侵的能力。

**参考答案**

（42）C

**试题（43）**

宏病毒可以感染后缀为__（43）__的文件。

（43）A．exe　　B．txt　　C．pdf　　D．xls

**试题（43）分析**

本题考查病毒的基本知识。

宏病毒是一种脚本病毒，宏病毒的前缀是 Macro，第二前缀是 Word、Word 97、Excel、Excel 97 等。宏病毒可以寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

因此，只有微软的 Word 文档或者 Excel 文档才会感染宏病毒。

**参考答案**

（43）D

**试题（44）**

Kerberos 是一种__（44）__。

（44）A．加密算法　　B．签名算法　　C．认证服务　　D．病毒

**试题（44）分析**

本题考查的是认证的基本知识。

Kerberos 是一项认证服务，它要解决的问题是：在公开的分布式环境中，工作站上的用户希望通过安全的方式访问分布在网络的服务器。

Kerberos 的设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

**参考答案**

（44）C

**试题（45）**

以下关于三重 DES 加密的叙述中，正确的是__（45）__。

（45）A．三重 DES 加密使用一个密钥进行三次加密

B．三重 DES 加密使用两个密钥进行三次加密

C．三重 DES 加密使用三个密钥进行三次加密

D．三重 DES 加密的密钥长度是 DES 密钥长度的 3 倍

**试题（45）分析**

本题考查的是三重 DES 加密的基本知识。

三重 DES 加密谁的 DES 加密算法的改进算法，它使用两把密钥对待加密报文作三次 DES 加密，其效果相当于将 DES 密钥的长度加倍，从而克服了 DES 密钥长度较短的缺点。其加密的过程如下：

假设两个密钥分别为 K1 和 K2，其加密过程是：

① 用密钥 *K*1 进行 DES 加密。

② 用 *K*2 对步骤①的结果进行 DES 解密。

③ 对步骤②的结果使用密钥 *K*1 进行 DES 加密。

**参考答案**

（45）B

**试题（46）**

SNMP 协议属于__（46）__层协议。

（46）A．物理　　B．网络　　C．传输　　D．应用

**试题（46）分析**

本题考查 SNMP 方面的基础知识。

SNMP 为应用层协议，是 TCP/IP 协议族的一部分。它通过用户数据报协议（UDP）来操作。在分立的管理站中，管理者进程对位于管理站中心的 MIB 的访问进行控制，并提供网络管理员接口。管理者进程通过 SNMP 完成网络管理。

**参考答案**

（46）D

**试题（47）**

SNMPv3 新增了__（47）__功能。

（47）A．管理站之间通信　　B．代理

C．认证和加密　　D．数据块检索

**试题（47）分析**

本题考查 SNMPv3 方面的基础知识。

SNMPv3 通过对数据进行认证和加密，确保数据在传输过程中不被篡改、确保数据从合法的数据源发出、加密报文，确保数据的机密性等安全特性。

**参考答案**

（47）C

**试题（48）**

网络管理系统中故障管理的目标是__（48）__。

（48）A．自动排除故障　　B．优化网络性能
　　C．提升网络安全　　D．自动监测故障

**试题（48）分析**

本题考查网络管理系统方面的基础知识。

ISO/IEC 7498-4 文档定义了网络管理的相关知识，其中故障管理的目标应包括：故障监测、故障报警、故障信息管理、排错支持工具、检索/分析故障信息等内容。

**参考答案**

（48）D

**试题（49）**

一台主机的浏览器无法访问域名为 www.sohu.com 的网站，并且在这台计算机执行 tracert 命令时有如下信息：

```
Tracing route to www.sohu.com [202.113.96.10]Over maximum of 30 hops:
 1 <1ms <1ms <1ms 59.67.148.1
 2 59.67.148.1 reports:Destination net unreachable
 Trace complete
```

根据以上信息，造成这种现象的原因可能是__（49）__。

（49）A．该计算机 IP 地址设置有误
　　B．相关路由器上进行了访问控制
　　C．本地网关不可达
　　D．本地 DNS 服务器工作不正常

**试题（49）分析**

本题考查网络管理命令 tracert 的使用及相关结果分析方面的基础知识。

59.67.148.1 是第 1 跳即网关，从返回的延迟信息可以看到到网关的连接很顺畅，排除了 A 和 C；再由输入的是域名 www.sohu.com 能正常地解析到地址 202.113.96.10，说明本地 DNS 服务器工作正常；到达网关之后到不了下 1 跳，极大可能是出口路由器上进行了访问控制。

**参考答案**

（49）B

**试题（50）**

使用 netstat -o 命令可显示网络__（50）__。

（50）A．IP、ICMP、TCP、UDP 协议的统计信息
　　B．以太网统计信息
　　C．以数字格式显示所有连接、地址及端口

D．每个连接的进程 ID

**试题（50）分析**

本题考查网络管理命令 netstat 的使用及相关参数的作用。

netstat 命令用于显示 TCP 连接。Netstat 命令的语法如下：

**netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *Protocol*] [**-r**] [**-s**] [*Interval*]

对以上参数解释如下：

- -a

显示所有活动的 TCP 连接，以及正在监听的 TCP 和 UDP 端口。

- -e

显示以太网统计信息，例如发送和接收的字节数，以及出错的次数等。这个参数可以与-s 参数联合使用。

- -n

显示活动的 TCP 连接，地址和端口号以数字形式表示。

- -o

显示活动的 TCP 连接以及每个连接对应的进程 ID。在 Windows 任务管理器中可以找到与进程 ID 对应的应用。这个参数可以与-a、-n 和-p 联合使用。

- -p *Protocol*

用标识符 Protocol 指定要显示的协议，可以是 TCP、UDP、TCPv6 或者 UDPv6。如果与参数-s 联合使用，则可以显示协议 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6 的统计数据。

- -s

显示每个协议的统计数据。默认情况下，统计 TCP、UDP、ICMP 和 IP 协议发送和接收的数据包、出错的数据包、连接成功或失败的次数等。如果与-p 参数联合使用，可以指定要显示统计数据的协议。

- -r

显示 IP 路由表的内容，其作用等价于路由打印命令 route print。

- *Interval*

说明重新显示信息的时间间隔，键入 Ctrl+C 则停止显示。如果不使用这个参数，则只显示一次。

**参考答案**

（50）D

**试题（51）**

IEEE 802.1x 是一种基于＿（51）＿认证协议。

（51）A．用户 ID　　　　B．报文

C．MAC 地址　　　　D．SSID

**试题（51）分析**

IEEE 802.1x 协议实现基于端口（MAC 地址）的访问控制。认证系统对连接到链路对端的请求者进行认证。一般在用户接入设备上实现 802.1x 认证。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

**参考答案**

（51）C

**试题（52）**

为了弥补 WEP 协议的安全缺陷，WPA 安全认证方案增加的机制是＿（52）＿。

（52）A. 共享密钥认证　　B. 临时密钥完整性协议

C. 较短的初始化向量　　D. 采用更强的加密算法

**试题（52）分析**

有线等效保密 WEP 的设计目的是提供与有线局域网等价的机密性。WEP 使用RC4协议进行加密，并使用CRC-32校验保证数据的完整性。

最初的 WEP 标准使用 24bit 的初始向量，加上 40bit的字符串，构成 64bit 的 WEP 密钥。后来美国政府也允许使用 104bit 的字符串，加上 24bit 的初始向量，构成 128bit 的 WEP 密钥。然而 24bit 的 IV 并没有长到足以保证不会出现重复，只要网络足够忙碌，在很短的时间内就会耗尽可用的 IV 而使其出现重复，这样 WEP 密钥也就重复了。

Wi-Fi联盟厂商以 802.11i 草案的子集为蓝图制定了称为WPA（Wi-Fi Protected Access）安全认证方案。在 WPA 的设计中包含了认证、加密和数据完整性校验三个组成部分。首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以 128bit 的密钥和 48 位的初始向量（IV）用于RC4加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议TKIP，以更频繁地变换密钥来减少安全风险。最后，WPA 强化了数据完整性保护，使用报文完整性编码来检测伪造的数据包，并且在报文认证码中包含有帧计数器，还可以防止重放攻击。

**参考答案**

（52）B

**试题（53）**

由 DHCP 服务器分配的默认网关地址是 192.168.5.33/28，＿（53）＿是本地主机的有效地址。

（53）A. 192.168.5.32　　B. 192.168.5.55

C. 192.168.5.47　　D. 192.168.5.40

**试题（53）分析**

默认网关地址 192.168.5.33/28 的二进制：**11000000.10101000. 00000101.0010**0001

192.168.5.32 的二进制：**11000000.10101000. 00000101.0010**0000 这是一个子网地址。

192.168.5.55 的二进制：**11000000.10101000. 00000101.0011**0111 这个地址与网关地址不在同一子网中。

192.168.5.47 的二进制：**11000000.10101000. 00000101.0010**1111 这是一个广播地址。

192.168.5.40 的二进制：**11000000.10101000. 00000101.0010**1000 这是本地主机的有效地址。

**参考答案**

（53）D

**试题（54）**

如果指定的地址掩码是 255.255.254.0，则有效的主机地址是__（54）__。

（54）A．126.17.3.0　　　　B．174.15.3.255

C．20.15.36.0　　　　D．115.12.4.0

**试题（54）分析**

地址掩码是 255.255.254.0，所以主机地址占最后的 9 位。

126.17.3.0 的二进制为：**01111110.00010001. 0000001**1.00000000 这是一个有效的主机地址。

174.15.3.255 的二进制：**10101110.00001111. 0000001**1.11111111 这是一个广播地址。

20.15.36.0 的二进制：**00010100.00001111. 0010010**0.00000000 这是一个子网地址。

115.12.4.0 的二进制：**01110011.00001100. 0000010**0.00000000 这也是一个子网地址。

**参考答案**

（54）A

**试题（55）**

如果要检查本机的 IP 协议是否工作正常，则应该 ping 的地址是__（55）__。

（55）A．192.168.0.1　　　　B．10.1.1.1

C．127.0.0.1　　　　D．128.0.1.1

**试题（55）分析**

要检查本机的 IP 协议是否工作正常，则应该 ping 的地址是 127.0.0.1，该地址在 Windows 中被称为本地回环地址（Loopback Address）。

**参考答案**

（55）C

**试题（56）**

工作站 A 的 IP 地址是 202.117.17.24/28，而工作站 B 的 IP 地址是 202.117.17.100/28，当两个工作站直接相连时不能通信，怎样修改地址才能使得这两个工作站可以互相通信？__（56）__。

（56）A．把工作站 A 的地址改为 202.117.17.15

B．把工作站 B 的地址改为 202.117.17.112

C．把子网掩码改为 25

D．把子网掩码改为 26

**试题（56）分析**

工作站 A 的 IP 地址是 202.117.17.24/28：**11001010.01110101. 00010001.0001**1000

工作站 B 的 IP 地址是 202.117.17.100/28：**11001010.01110101. 00010001.0110**1000

当前的这两个地址不属于同一个子网，把地址掩码改为 25 就属于同一个子网了。

**参考答案**

（56）C

**试题（57）**

运营商指定本地路由器接口的地址是 200.15.10.6/29，路由器连接的默认网关的地址是 200.15.10.7，这样配置后发现路由器无法 ping 通任何远程设备，原因是__（57）__。

（57）A．默认网关的地址不属于这个子网

B．默认网关的地址是子网中的广播地址

C．路由器接口地址是子网中的广播地址

D．路由器接口地址是组播地址

**试题（57）分析**

本地路由器接口的地址 200.15.10.6/29：**11001000.00001111. 00001010.00000**110

默认网关的地址 200.15.10.7：**11001000.00001111. 00001010.00000**111

默认网关的地址是广播地址。

**参考答案**

（57）B

**试题（58）**

访问控制列表（ACL）配置如下，如果来自因特网的 HTTP 报文的目标地址是 162.15.10.10，经过这个 ACL 过滤后会出现什么情况？__（58）__

```
Router#show access-lists
Extended IP access list 110
    10 deny tcp 162.15.0.0 0.0.255.255 any eq telnet
    20 deny tcp 162.15.0.0 0.0.255.255 any eq smtp
    30 deny tcp 162.15.0.0 0.0.255.255 any eq http
    40 permit tcp 162.15.0.0 0.0.255.255 any
```

（58）A．由于行 30 拒绝，报文被丢弃

B．由于行 40 允许，报文被接受

C．由于 ACL 末尾隐含的拒绝，报文被丢弃

D．由于报文源地址未包含在列表中，报文被接受

**试题（58）分析**

语句 10 deny tcp 162.15.0.0 0.0.255.255 any eq telnet 的作用是拒绝来自 162.15.0.0 网络的 telnet 访问。

语句 20 deny tcp 162.15.0.0 0.0.255.255 any eq smtp 的作用是拒绝来自 162.15.0.0 网络的 smtp 访问。

语句 30 deny tcp 162.15.0.0 0.0.255.255 any eq http 的作用是拒绝来自 162.15.0.0 网络的 http 访问。来自因特网的目标地址是 162.15.10.10 的 http 报文不能被这个语句过滤。

语句 40 permit tcp 162.15.0.0 0.0.255.255 any 的作用是允许来自 162.15.0.0 网络的任何访问。这个语句也不会过滤来自因特网的目标地址是 162.15.10.10 的 http 报文。

所以来自因特网的目标地址是 162.15.10.10 的 http 报文被 ACL 末尾隐含的拒绝语句阻止，报文被丢弃。

**参考答案**

（58）C

**试题（59）**

下面的 4 个 IPv6 地址中，无效的地址是__（59）__。

（59）A．: :192:168:0:1　　　B．2001:3452:4955:2367: :

　　C．2002:c0a8:101::43　　　D．2003:dead:beef:4dad:23:34:bb:101

**试题（59）分析**

4 个 IPv6 地址中，无效的地址是 B．2001:3452:4955:2367: :，最后一对冒号的写法是错误的，其他 3 种写法都正确。: :192:168:0:1 是一个 IPv4 地址，2002:c0a8:101::43 中的双冒号表示 4 个双字节，2003:dead:beef:4dad:23:34:bb:101 是完整的 IPv6 地址。

**参考答案**

（59）B

**试题（60）**

IPv6 站点通过 IPv4 网络通信需要使用隧道技术，常用的 3 种自动隧道技术是__（60）__。

（60）A．VPN 隧道、PPTP 隧道和 IPsec 隧道

　　B．6to4 隧道、6over4 隧道和 ISATAP 隧道

　　C．VPN 隧道、PPP 隧道和 ISATAP 隧道

　　D．IPsec 隧道、6over4 隧道和 PPTP 隧道

**试题（60）分析**

IPv6 站点通过 IPv4 网络通信，最常用的 3 种自动隧道技术是 6to4 隧道、6over4 隧道和 ISATAP 隧道。

**参考答案**

（60）B

**试题（61）**

如果在网络的入口处通过设置 ACL 封锁了 TCP 和 UDP 端口 21、23 和 25，则能够访问该网络的应用是__（61）__。

（61）A．FTP　　B．DNS　　C．SMTP　　D．Telnet

**试题（61）分析**

由于 TCP 和 UDP 端口 21、23 和 25 被封锁，它们分别是 FTP、Telnet 和 SMTP 的端口号，所以只有 DNS 应用可以访问该网络。

**参考答案**

（61）B

**试题（62）**

以太网采用物理地址的目的是__（62）__。

（62）A．唯一地标识第二层设备

B．使得不同网络中的设备可以互相通信

C．用于区分第二层的帧和第三层的分组

D．物理地址比网络地址的优先级高

**试题（62）分析**

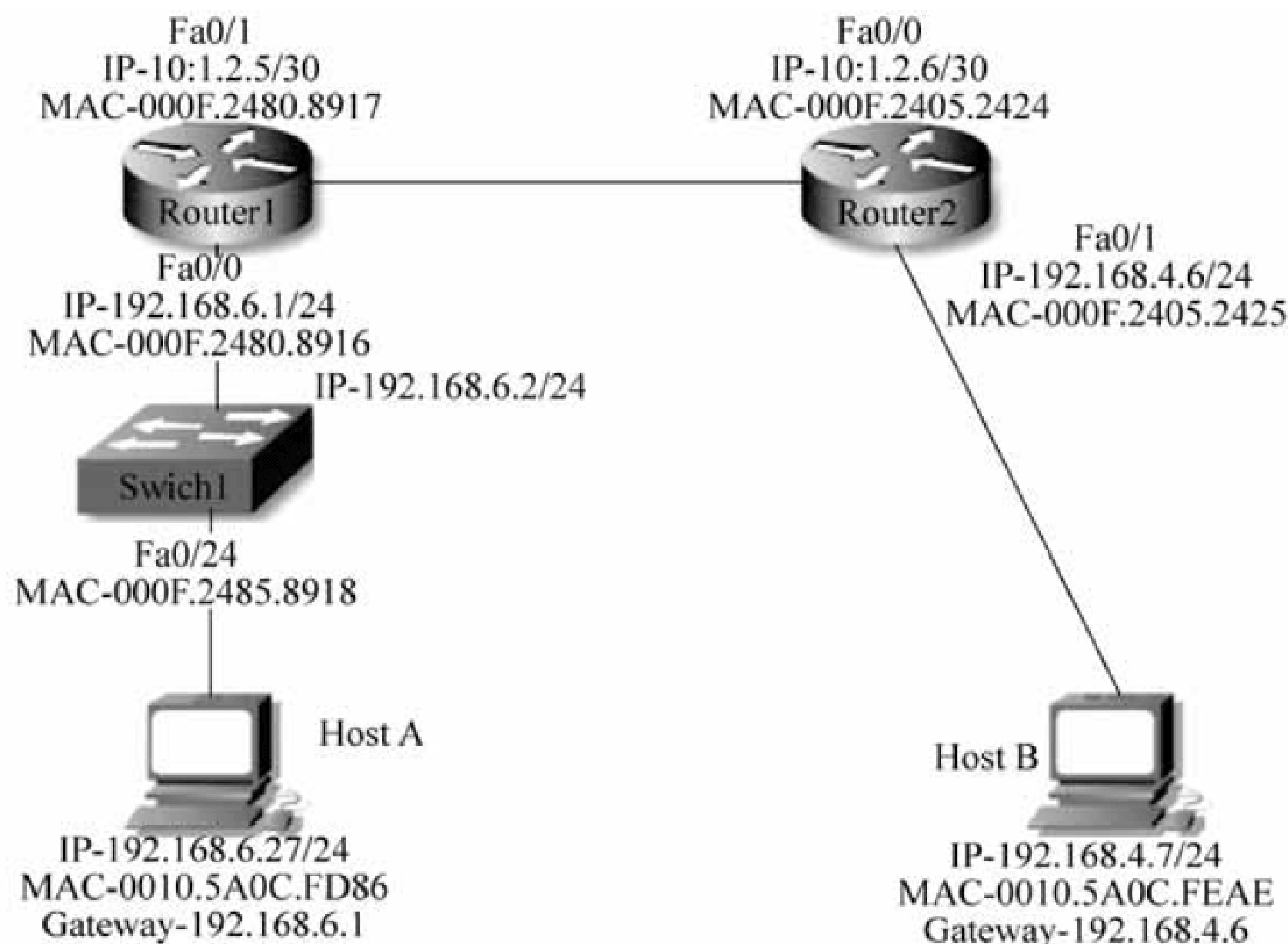
以太网物理地址（即 MAC 地址）是第二层设备的唯一标识。

**参考答案**

（62）A

**试题（63）**

参见下面的网络连接图，4 个选项是 HostA 的 ARP 表，如果 HostA ping HostB，则 ARP 表中的哪一选项用来封装传输的帧？__（63）__



(63)

| | Interface Address | Physical Address | Type |
|---|---|---|---|
| A. | 192.168.4.7 | 000f 2480 8916 | dynamic |
| B. | 192.168.4.7 | 0010 5a0c feae | dynamic |
| C. | 192.168.6.2 | 0010 5a0c feae | dynamic |
| D. | 192.168.6.1 | 000f 2480 8916 | dynamic |

**试题（63）分析**

在 HostA 处组成的分组应该以 HostB 的 IP 地址 192.168.4.7 为目标地址，查找本地 ARP 表，得到的不是 HostB 的 MAC 地址，而是边界路由器的 MAC 地址 000f 2480 8916，所以 HostA 装配成帧时只能以边界路由器的 MAC 地址为目标地址。这就是说，路由器以自己的 MAC 地址代理了目标主机 HostB 的 MAC 地址，这就是代理 ARP 的概念，当两个主机不属于同一子网时，必须借助于这种机制才能互相通信。

**参考答案**

（63）D

**试题（64）**

4G 移动通信标准 TD-LTE 与 FDD-LTE 的区别是__（64）__。

（64）A．频率的利用方式不同　　B．划分上下行信道的方式不同

C．采用的调制方式有区别　　D．拥有专利技术的厂家不同

**试题（64）分析**

4G 移动通信标准 TD-LTE（即 TDD-LTE）与 FDD-LTE 的主要区别是划分上下行信道的方式不同，前者用时分多路方式，而后者用频分多路方式。其他方面大同小异。

**参考答案**

（64）B

**试题（65）**

关于移动 Ad Hoc 网络 MANET，__（65）__不是 MANET 的特点。

（65）A．网络拓扑结构是动态变化的

B．电源能量限制了无线终端必须以最节能的方式工作

C．可以直接应用传统的路由协议支持最佳路由选择

D．每一个结点既是主机又是路由器

**试题（65）分析**

在移动 Ad Hoc 网络 MANET 中，每一个结点既是主机又是路由器，而且无线终端所带的电源能量有限，所以必须以最节能的方式工作。由于无线终端的移动，使得网络拓扑结构随时变化，传统的路由协议是不适用的，必须采用特别研制路由协议来支持最佳路由的选择。

**参考答案**

（65）C

**试题（66）**

（66）针对 TCP 连接进行攻击。

（66）A．拒绝服务　　B．暴力攻击

C．网络侦察　　D．特洛伊木马

**试题（66）分析**

拒绝服务主要是针对 TCP 连接进行攻击的，通过发送大量的建立连接请求，使得服务端穷于应付，无法提供正常的网络服务。暴力攻击是穷举式猜测用户密码。网络侦察是探测远端系统的漏洞，以便利用漏洞进行入侵。特洛伊木马是通过远端控制，对目标系统实施内部破坏或盗窃用户机密数据。

**参考答案**

（66）A

**试题（67）、（68）**

安全需求可划分为物理安全、网络安全、系统安全和应用安全，下面的安全需求中属于系统安全的是（67），属于应用安全的是（68）。

（67）A．机房安全　　B．入侵检测

C．漏洞补丁管理　　D．数据库安全

（68）A．机房安全　　B．入侵检测

C．漏洞补丁管理　　D．数据库安全

**试题（67）、（68）分析**

机房安全属于物理安全，入侵检测属于网络安全，漏洞补丁管理属于系统安全，而数据库安全则是应用安全。

**参考答案**

（67）C　（68）D

**试题（69）**

一个中等规模的公司，3 个不同品牌的路由器都配置了 RIPv1 协议。ISP 为公司分配的地址块为 201.113.210.0/24。公司希望通过 VLSM 技术把网络划分为 3 个子网，每个子网中有 40 台主机，下面的配置方案中最优的是（69）。

（69）A．转换路由协议为 EIGRP，3 个子网地址分别设置为 201.113.210.32/27、201.113.210.64/27 和 201.113.210.92/27

B．转换路由协议为 RIPv2，3 个子网地址分别设置为 201.113.210.64/26、201.113.210.128/26 和 201.113.210.192/26

C．转换路由协议为 OSPF，3 个子网地址分别设置为 201.113.210.16/28、201.113.210.32/28 和 201.113.210.48/28

D．保持路由协议为 RIPv1，3 个子网地址分别设置为 201.113.210.32/26、201.113.210.64/26 和 201.113.210.92/26

**试题（69）分析**

每个子网中有 40 台主机，所以主机地址要占用 6 位，因而子网掩码必须是 26 位，同时把路由协议由 RIPv1 转换为 RIPv2，它是无类别的协议（Classless Protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR）。

**参考答案**

（69）B

**试题（70）**

如果发现网络的数据传输很慢，服务质量也达不到要求，应该首先检查哪一个协议层工作情况？__（70）__

（70）A．物理层　　B．会话层　　C．网络层　　D．传输层

**试题（70）分析**

如果网络的数据传输很慢，服务质量也达不到要求，通常先要检查网络层工作是否正常。

**参考答案**

（70）C

**试题（71）～（75）**

Traditional network layer packet forwarding relies on the information provided by network layer __（71）__ protocols, or static routing, to make an independent forwarding decision at each __（72）__ within the network. The forwarding decision is based solely on the destination __（73）__ IP address. All packets for the same destination follow the same path across the network if no other equal-cost __（74）__ exist. Whenever a router has two equal-cost paths toward a destination, the packets toward the destination might take one or both of them, resulting in some degree of load sharing. Enhanced Interior Gateway Routing Protocol (EIGRP) also supports non–equal-cost __（75）__ sharing although the default behavior of this protocol is equal-cost. You must configure EIGRP variance for non–equal-cost load balancing.

（71）A．switching　　B．signaling　　C．routing　　D．session
（72）A．switch　　B．hop　　C．host　　D．customer
（73）A．connection　　B．transmission　　C．broadcast　　D．unicast
（74）A．paths　　B．distance　　C．speed　　D．session
（75）A．loan　　B．load　　C．content　　D．constant

**参考译文**

传统的网络层分组转发是根据网络层路由协议或者静态路由提供的信息，在网络中的每一跳都做出一个独立的转发决策。转发决策只是基于目标单播地址而做出的。如果

没有相等费用的其他通路存在，朝着同一目标的所有分组都遵循网络中的同样路径。当路由器具有通向同一目标的相等费用的两条通路时，流向目标的分组就可能走两条通路中的任何一条，这就产生了同样程度的负载共享。增强的内部网关路由协议（EIGRP）也支持不等费用的负载共享，虽然这个协议默认的行为是相等费用的负载共享。通过配置，你可以把 EIGRP 变成不等费用的负载共享方式。

**参考答案**

（71）C （72）B （73）D （74）A （75）B

# 第 26 章　2015 上半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业网络拓扑图如图 1-1 所示。

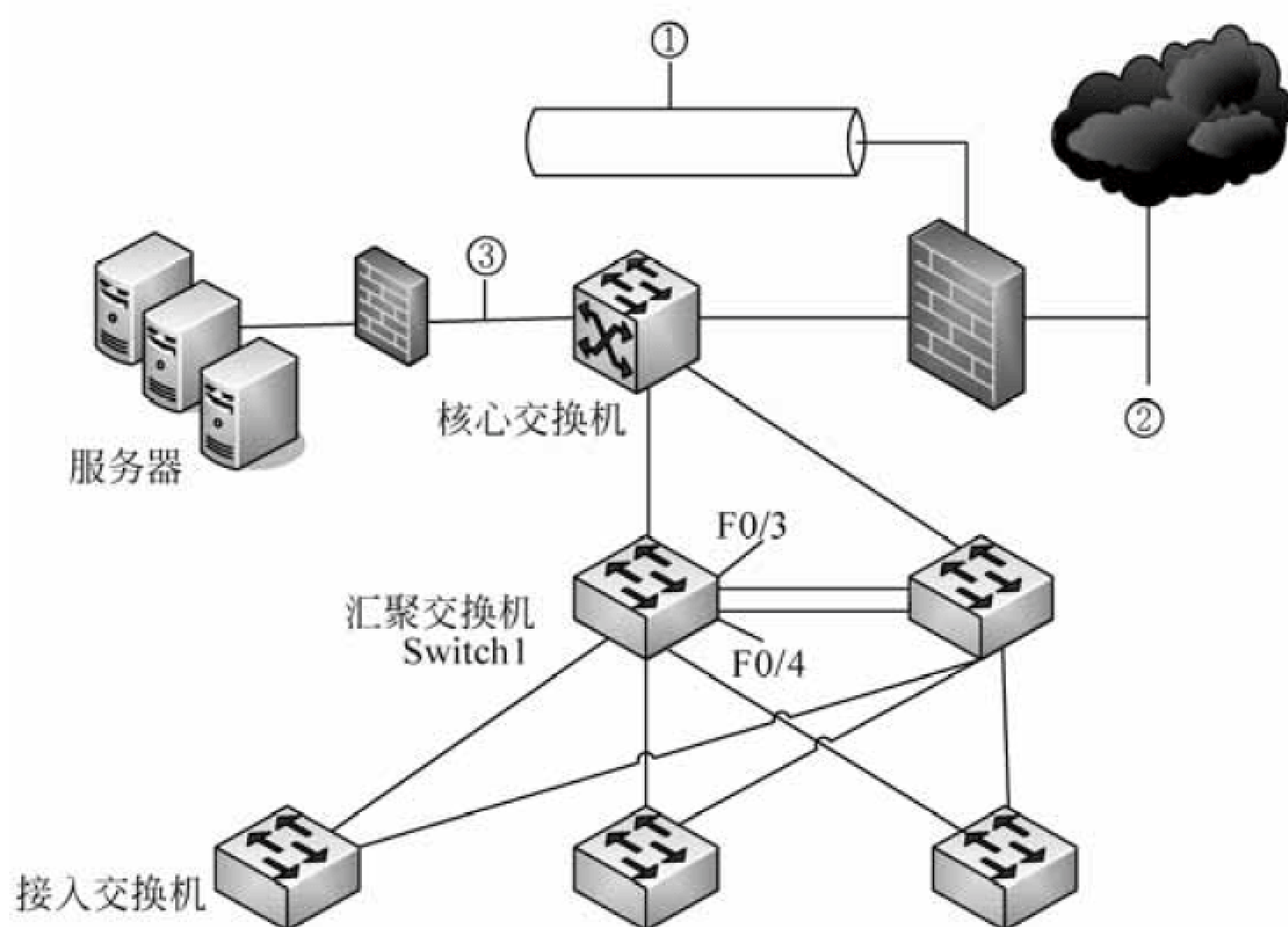



图 1-1

工程师给出了该网络的需求：

1．用防火墙实现内外网地址转换和访问控制策略；

2．核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；

3．接入层到汇聚层采用双链路方式组网；

4．接入层交换机对地址进行 VLAN 划分；

5．对企业的核心资源加强安全防护。

**【问题 1】（4 分）**

该企业计划在①、②或③的位置部署基于网络的入侵检测系统（NIDS），将 NIDS 部署在①的优势是 ___（1）___；将 NIDS 部署在②的优势是 ___（2）___、___（3）___；将 NIDS 部署在③的优势是 ___（4）___。

（1）～（4）备选答案：

A．检测外部网络攻击的数量和类型

B．监视针对 DMZ 中系统的攻击

C．监视针对关键系统、服务和资源的攻击

D．能减轻拒绝服务攻击的影响

**【问题 2】（4 分）**

OSPF 主要用于大型、异构的 IP 网络中，是对__（5）__路由的一种实现。若网络规模较小，可以考虑配置静态路由或__（6）__协议实现路由选择。

（5）备选答案：

A．链路状态　　B．距离矢量　　C．路径矢量

（6）备选答案：

A．EGP　　B．RIP　　C．BGP

**【问题 3】（4 分）**

对汇聚层两台交换机的 F0/3、F0/4 端口进行端口聚合，F0/3、F0/4 端口默认模式是__（7）__，进行端口聚合时应配置为__（8）__模式。

（7）、（8）备选答案：

A．multi　　B．trunk　　C．access

**【问题 4】（6 分）**

为了在汇聚层交换机上实现虚拟路由冗余功能，需配置__（9）__协议，可以采用竞争的方式选择主路由设备，比较设备优先级大小，优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文，则将自己的状态转为__（10）__。

为了避免二层广播风暴，需要在接入与汇聚设备上配置__（11）__。

（10）、（11）备选答案：

A．Master　　B．Backup　　C．VTP Server　　D．MSTP

**【问题 5】（2 分）**

阅读汇聚交换机 Switch1 的部分配置命令，回答下面的问题。

```
Switch1 (config)#interface vlan 20
Switch1 (config-if)#ip address 192.168.20.253 255.255.255.0
Switch1 (config-if)#standby 2 ip 192.168.20.250
Switch1 (config-if)#standby 2 preempt
Switch1 (config-if)#exit
```

VLAN20 的 standby 默认优先级的值是__（12）__。

VLAN20 设置 preempt 的含义是__（13）__。

**试题一分析**

本题考查网络规划以及组网的相关基础知识。包括入侵检测系统部署的技术规范，企业组网中路由协议的选用、线路聚合、生成树协议等相关知识。

【问题 1】

入侵检测系统（IDS）可以基于主机部署也可以基于网络进行部署，将 IDS 部署在网络中不同的位置区域可以达到对网络中异常行为和攻击的识别，对特定网络区域的资源进行保护。例如，将 IDS 部署在网络出口常用于监测外部网络攻击的数量和类型。

【问题 2】

路由器提供了异构网互联的机制，实现将一个网络的数据包发送到另一个网络。而路由就是指导 IP 数据包发送的路径信息。路由协议就是在路由指导 IP 数据包发送过程中事先约定好的规定和标准。常见的路由协议分为动态路由和静态路由，而动态路由协议又距离矢量路由协议和链路状态路由协议。

OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。

【问题 3】

端口聚合也叫作以太通道（Ethernet Channel），主要用于交换机之间连接。由于两个交换机之间有多条冗余链路的时候，STP 会将其中的几条链路关闭，只保留一条，这样可以避免二层的环路产生。

同一个汇聚组中端口的基本配置应该保持一致，即如果某端口为 trunk 端口，则其他端口也配置为 trunk 端口；如该端口的链路类型改为 access 端口，则其他端口的链路类型也改为 access 端口。

【问题 4】

汇聚交换机采用虚拟路由冗余，目的是当一台汇聚交换机出现故障时，启用备份线路的措施。根据设备情况可以采用虚拟路由器冗余协议（VRRP）或热备份路由器协议（HSRP）。

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

【问题 5】

HSRP 协议利用优先级决定哪个路由器成为活动路由器。如果一个路由器的优先级比其他路由器的优先级高，则该路由器成为活动路由器，路由器的默认优先级是 100。

当在交换机上配置链路冗余或负载均衡后，保证故障设备恢复后正常工作，需要设置 preempt 模式。

**参考答案**

【问题 1】

（1）B

（2）、（3）A　D

（4）C

【问题 2】

（5）A

（6）B

【问题 3】

（7）C

（8）B

【问题 4】

（9）VRRP 或者 HSRP

（10）A

（11）D

【问题 5】

（12）100

（13）设置为抢占模式，或交换机故障恢复后抢占 vlan20 的控制权。

**试题二（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司内部搭建了一个小型的局域网，拓扑图如图 2-1 所示。公司内部拥有主机约 120 台，用 C 类地址段 192.168.100.0/24。采用一台 Linux 服务器作为接入服务器，服务器内部局域网接口地址为 192.198.100.254，ISP 提供的地址为 202.202.212.62。

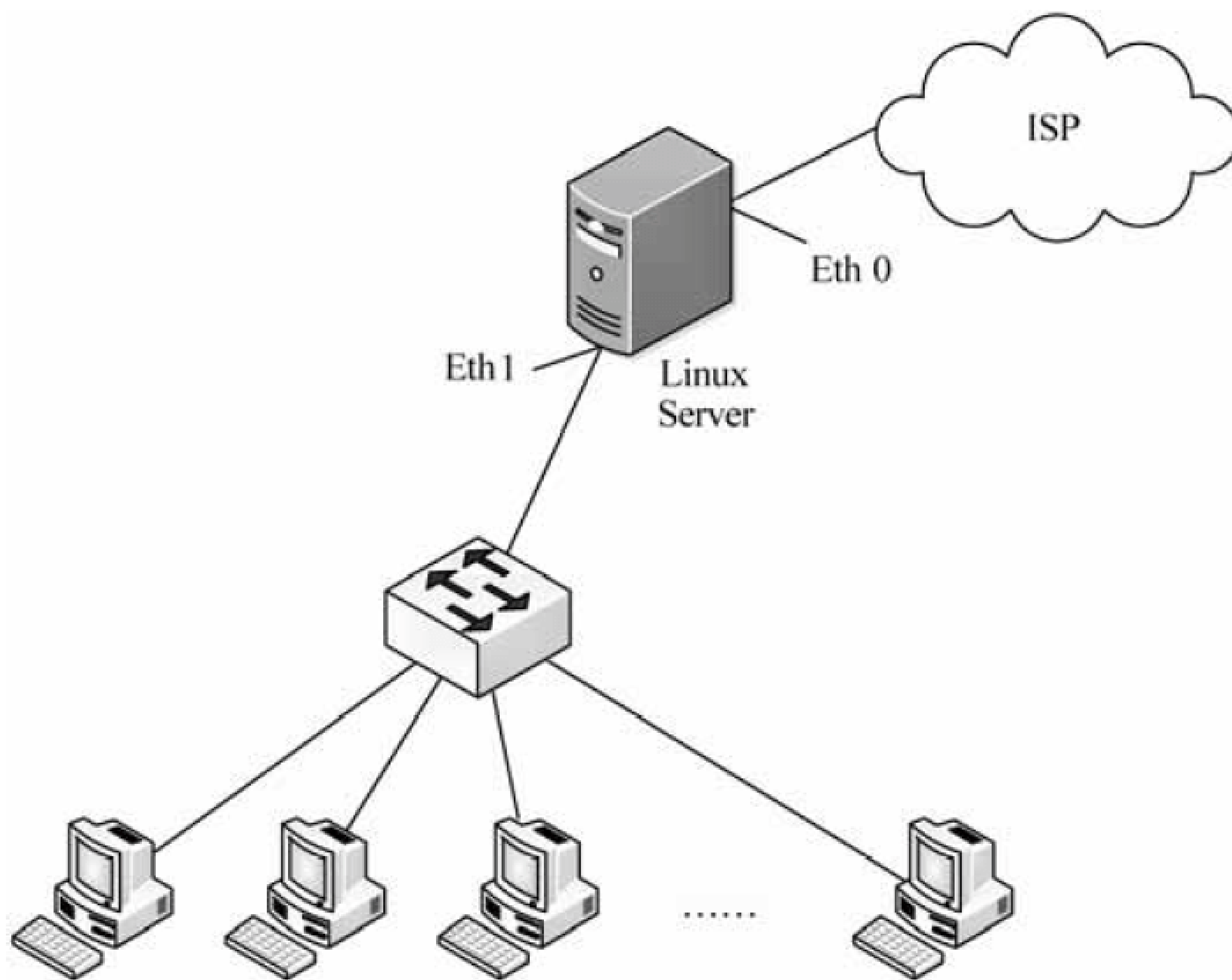



图 2-1

【问题 1】（2 分）

在 Linux 中，DHCP 的配置文件是 （1） 。

【问题 2】（8 分）

内部邮件服务器 IP 地址为 192.168.100.253，MAC 地址为 01:A8:71:8C:9A:BB；内

部文件服务器 IP 地址为 192.168.100.252，MAC 地址为 01:15:71:8C:77:BC。公司内部网络分为 4 个网段。

为方便管理，公司使用 DHCP 服务器为客户机动态配置 IP 地址，下面是 Linux 服务器为 192.168.100.192/26 子网配置 DHCP 的代码，将其补充完整。

```
Subnet__(2)__netmask __(3)__
{
    option routers 192.168.100.254;
    option subnet-mask __(4)__;
    option broadcast-address __(5)__;

    option time-offset -18000;

    range __(6)__ __(7)__;
    default-lease-time 21600;
    max-lease-time 43200;
        host servers
       {
        hardware ethernet __(8)__;
        fixed-address 192.168.100.253;
        hardware ethernet 01:15:71:8C:77:BC;
        fixed-address __(9)__;
       }
}
```

**【问题 3】（2 分）**

配置代码中"option time-offset -18000"的含义是__（10）__。"default-lease-time 21600"表明，租约期为__（11）__小时。

（10）备选答案：

A．将本地时间调整为格林威治时间

B．将格林威治时间调整为本地时间

C．设置最长租约期

**【问题 4】（3 分）**

在一台客户机上使用 ipconfig 命令输出如图 2-2 所示，正确的说法是__（12）__。

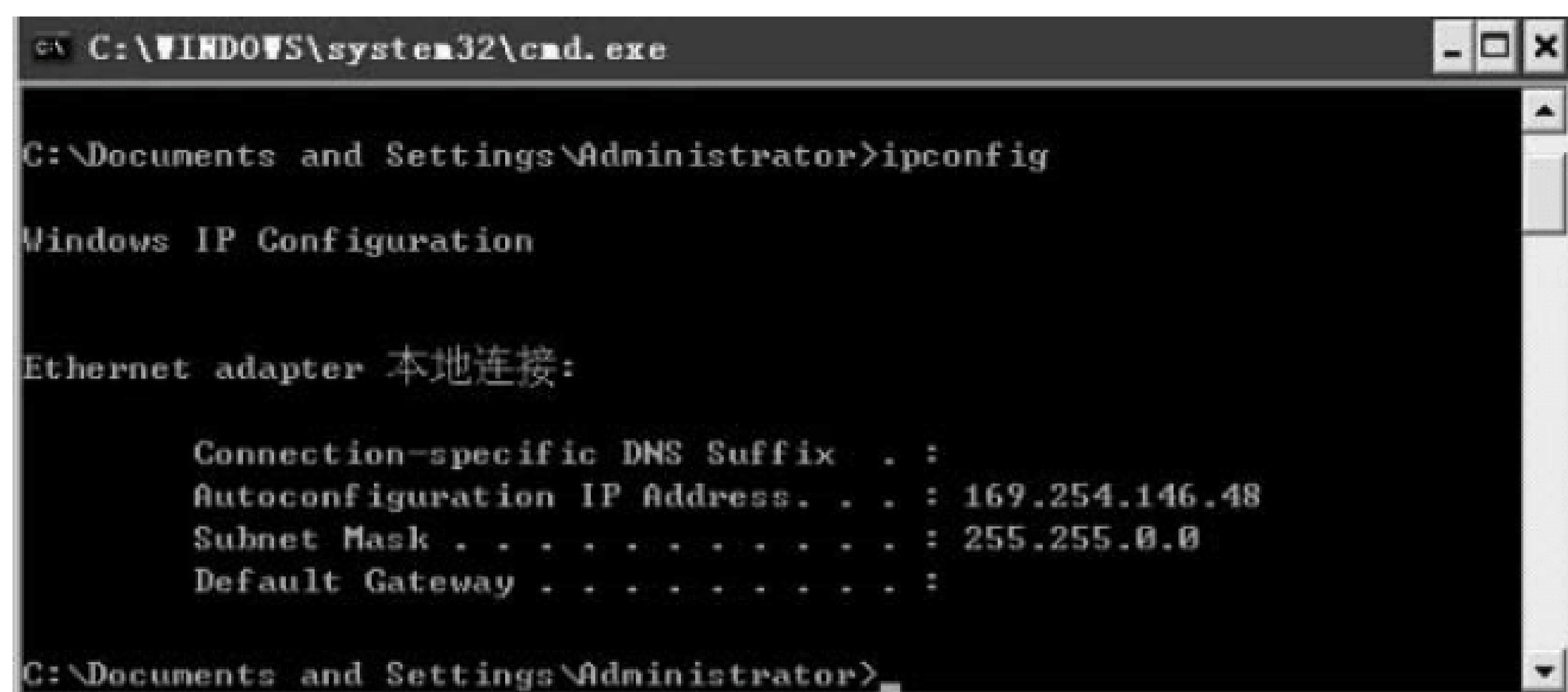



图 2-2

此时可使用＿（13）＿命令释放当前 IP 地址，然后使用＿（14）＿命令向 DHCP 服务器重新申请 IP 地址。

（12）备选答案：

A．本地网卡驱动未成功安装

B．未收到 DHCP 服务器分配的地址

C．DHCP 服务器分配给本机的 IP 地址为 169.254.146.48

D．DHCP 服务器的 IP 地址为 169.254.146.48

**试题二分析**

本题考查 Linux 服务器下 DHCP 服务器的配置。

**【问题 1】**

DHCP 服务是一种动态的为客户端主机分配 IP 地址的服务，在 Linux 服务器中，该服务的配置文件是 dhcp.conf。

**【问题 2】**

问题中给出了该公司所使用的 IP 地址所在子网为 192.168.100.192/26，网络号为 192.168.100.192，子网掩码为 255.255.255.192。本网的广播地址是将本网段中所有主机部分的二进制位数全部变为 1 得到，为 192.168.100.255。

空(6)和空(7)是要求计算该子网的 IP 地址范围，其有效的 IP 地址为 192.168.100.193 -192.168.100.254。

空（8）和空（9）按照问题的描述，要求填写对应的硬件地址和 IP 地址。

**【问题 3】**

option time-offset -18000 的配置项，是为了使得本地的 DHCP 服务器时间采用本地的时间进行计时，将从时间服务器中获取的格林威治时间调整到与本地时间同步的目的。default-lease-time 21600 的配置项是设置 IP 地址分配给客户端后的失效时间，改时间以秒为单位，即时间为 12600 秒，将其换算为小时的方法是 216000 秒/3600 秒=6 小时。

**【问题 4】**

图中所示的故障，是由于该客户端并未接收到系统的 DHCP 服务器所发来的 IP 地址配置信息，而有 TCP/IP 协议集为该客户端分配的 169.254.x.x 段的地址。169.254.x.x 地址是 IANA 组织规定的保留地址，为了未采用 DHCP 服务器动态分配 IP 地址的用户，当未获取 DHCP 分配的 IP 地址时，自动使用该段地址，该段地址一般不能使网络正常运行。

**参考答案**

**【问题 1】**

（1）dhcpd.conf

**【问题 2】**

（2）192.168.100.192

（3）255.255.255.192

（4）255.255.255.192

（5）192.168.100.255

（6）192.168.100.193

（7）192.168.100.251

（8）01:A8:71:8C:9A:BB

（9）192.168.100.252

**【问题 3】**

（10）B

（11）6

**【问题 4】**

（12）B

（13）ipconfig /release

（14）ipconfig /renew

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业在采用 Windows Server 2003 配置了共享打印、FTP 和 DHCP 服务。

**【问题 1】（8 分）**

1．Internet 共享打印使用的协议是＿（1）＿。

（1）备选答案：

A．PPI　　B．IPP　　C．TCP　　D．IP

2．Internet 共享打印配置完成后，需在如图 3-1 所示的 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”，其目的是＿（2）＿。

3．检验 Internet 打印服务是否安装正确的方法是在 Web 浏览器的地址栏输入 URL 是＿（3）＿。

（3）备选答案：

A．HTTP：//127.0.0.1/PRINTERS

B．FTP：//127.0.0.1/PRINTERS

C．HTTP：//PRINTERS

D．FTP：//PRINTERS

4．使用 Internet 共享打印流程为 6 个步骤：

① 在终端上输入打印设备的 URL；

② 服务器向用户显示打印机状态信息；

③ 客户端向打印服务器发送身份验证信息；

④ 用户把要打印的文件发送到打印服务器；

⑤ 打印服务器生成一个 cabinet 文件，下载到客户端；

⑥ 通过 Internet 把 HTTP 请求发送到打印服务器。

对以上步骤进行正确的排序＿（4）＿。

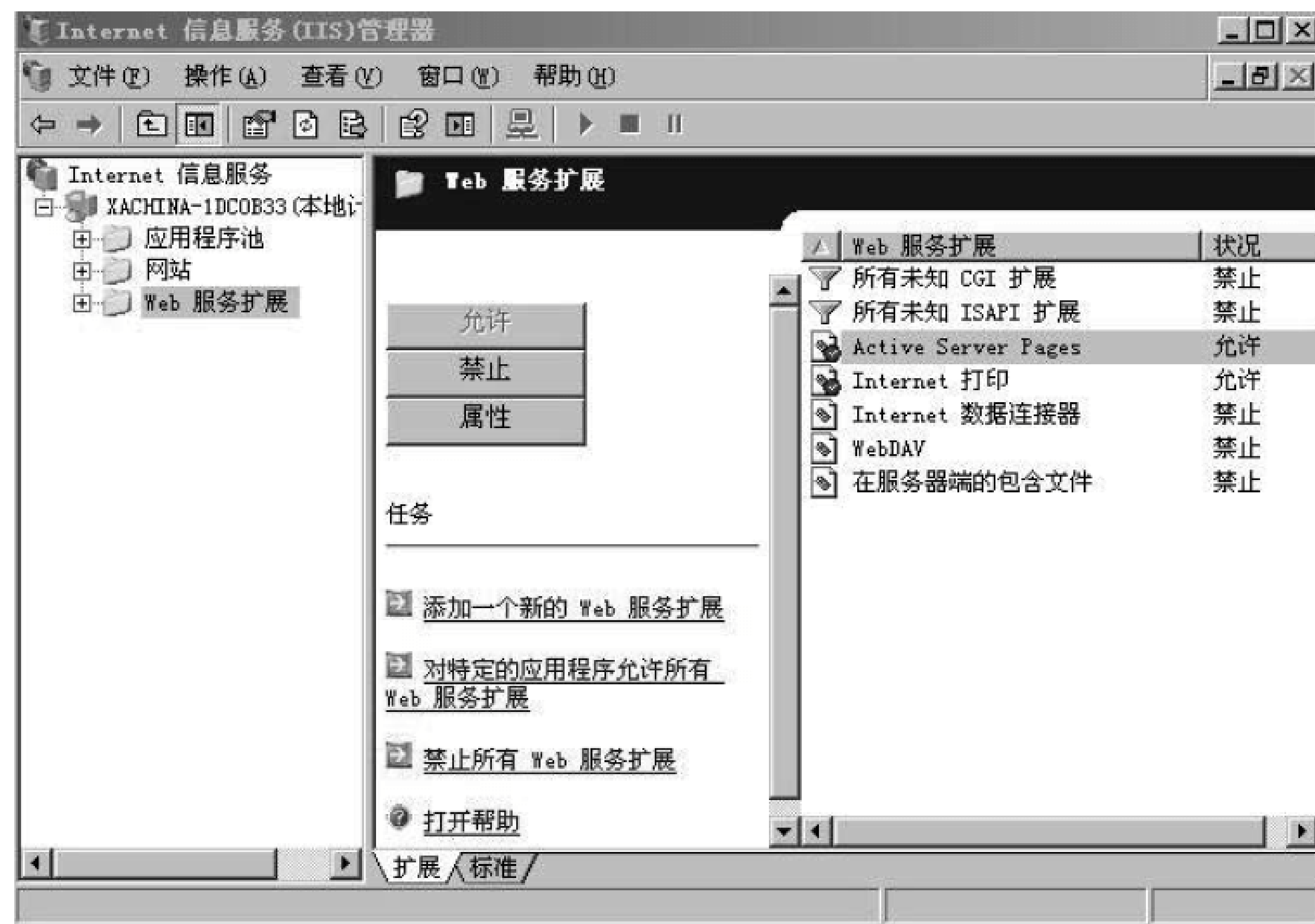



图 3-1

**【问题 2】（8 分）**

FTP 的配置如图 3-2、图 3-3 所示。

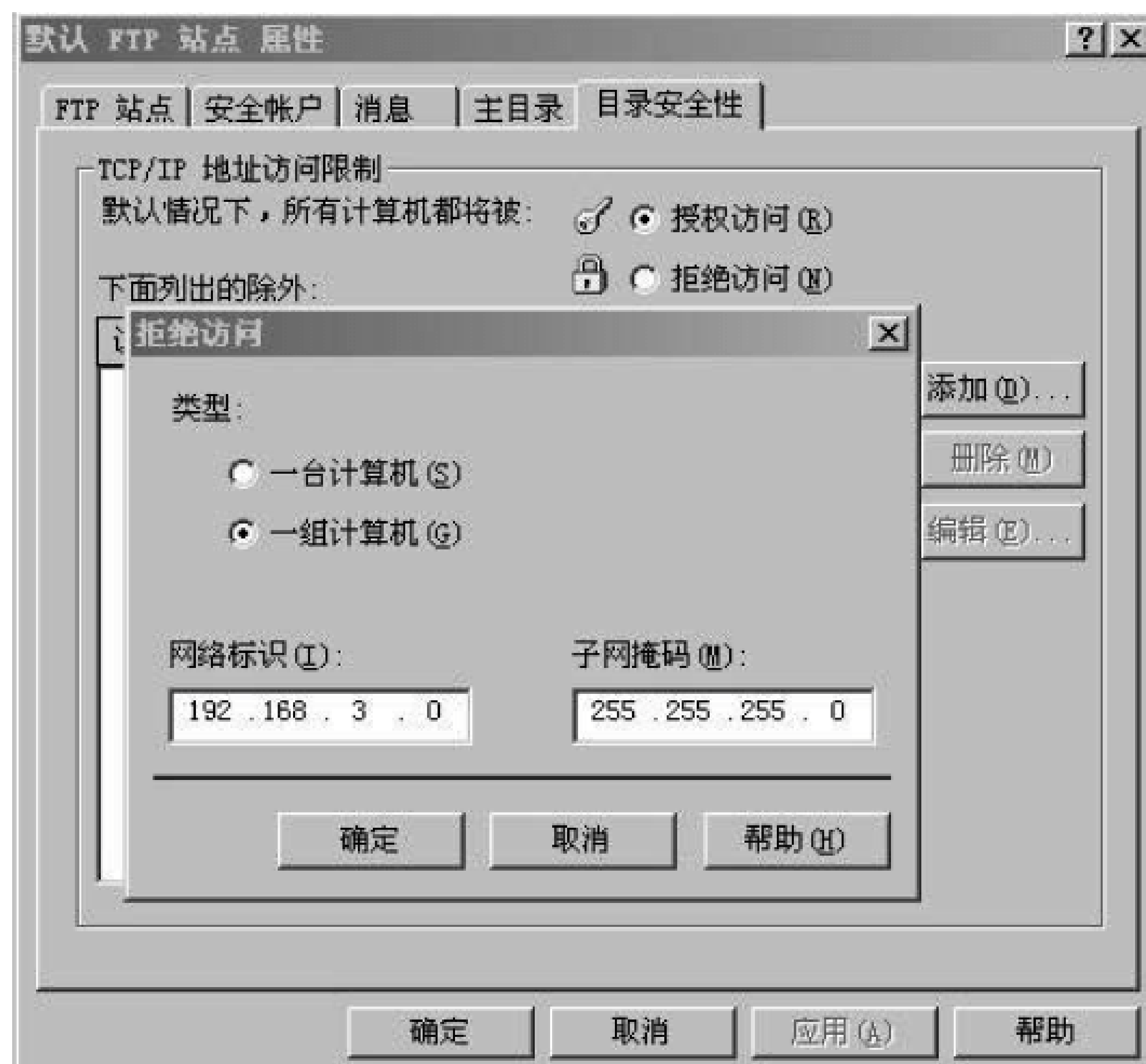



图 3-2

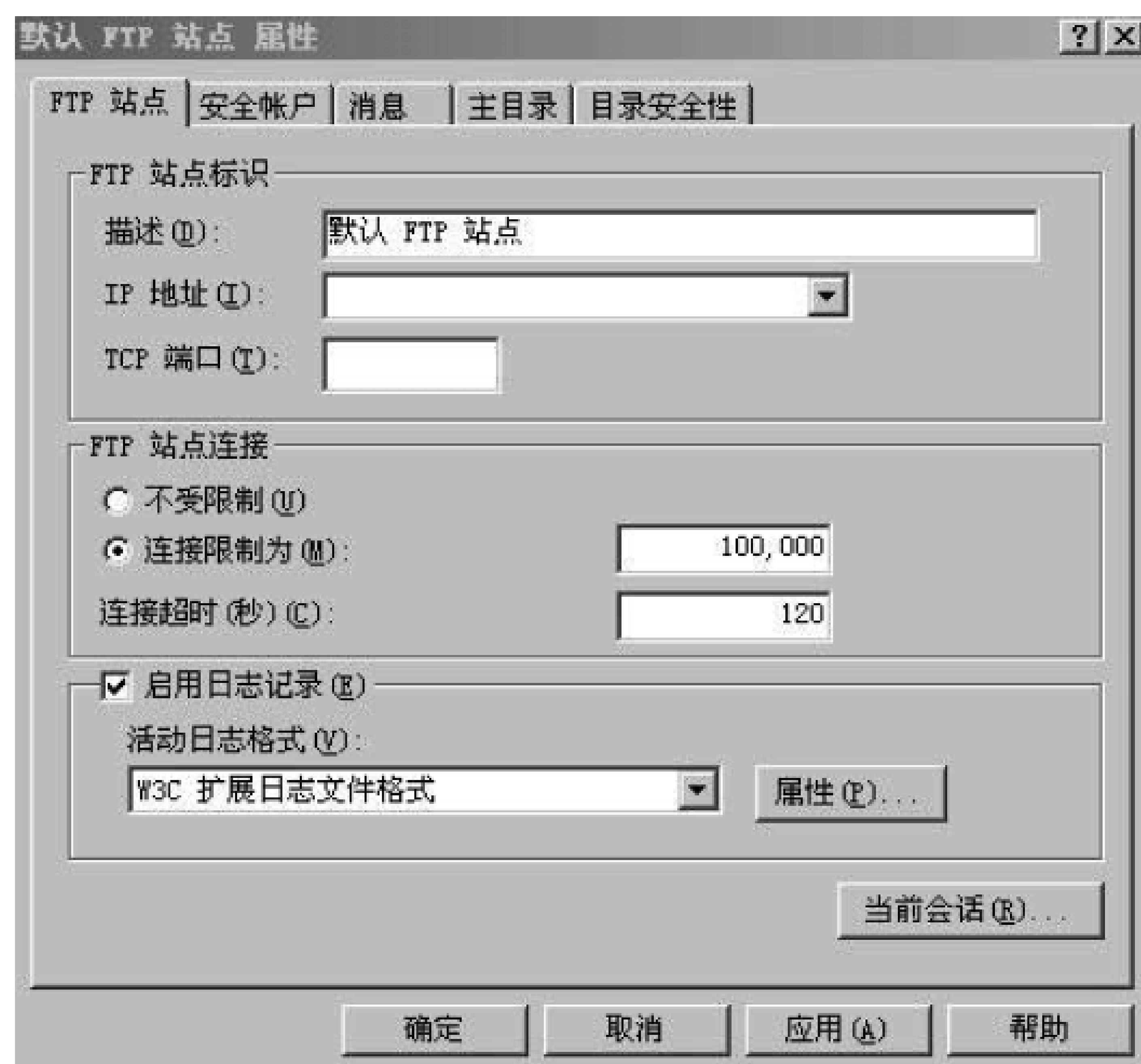



图 3-3

1. 默认情况下，用户登录 FTP 服务器时，服务器端建立的 TCP 端口号为＿（5）＿。
2. 如果只允许一台主机访问 FTP 服务器，参考图 3-2 给出具体的操作步骤＿（6）＿。
3. 参考图 3-3，在一台服务器上搭建多个 FTP 站点的方法是＿（7）＿。
4. 如单击图 3-3 中“当前会话”按钮，显示的信息是＿（8）＿。

**【问题 3】（4 分）**

DHCP 的配置如图 3-4 和图 3-5 所示。




图 3-4

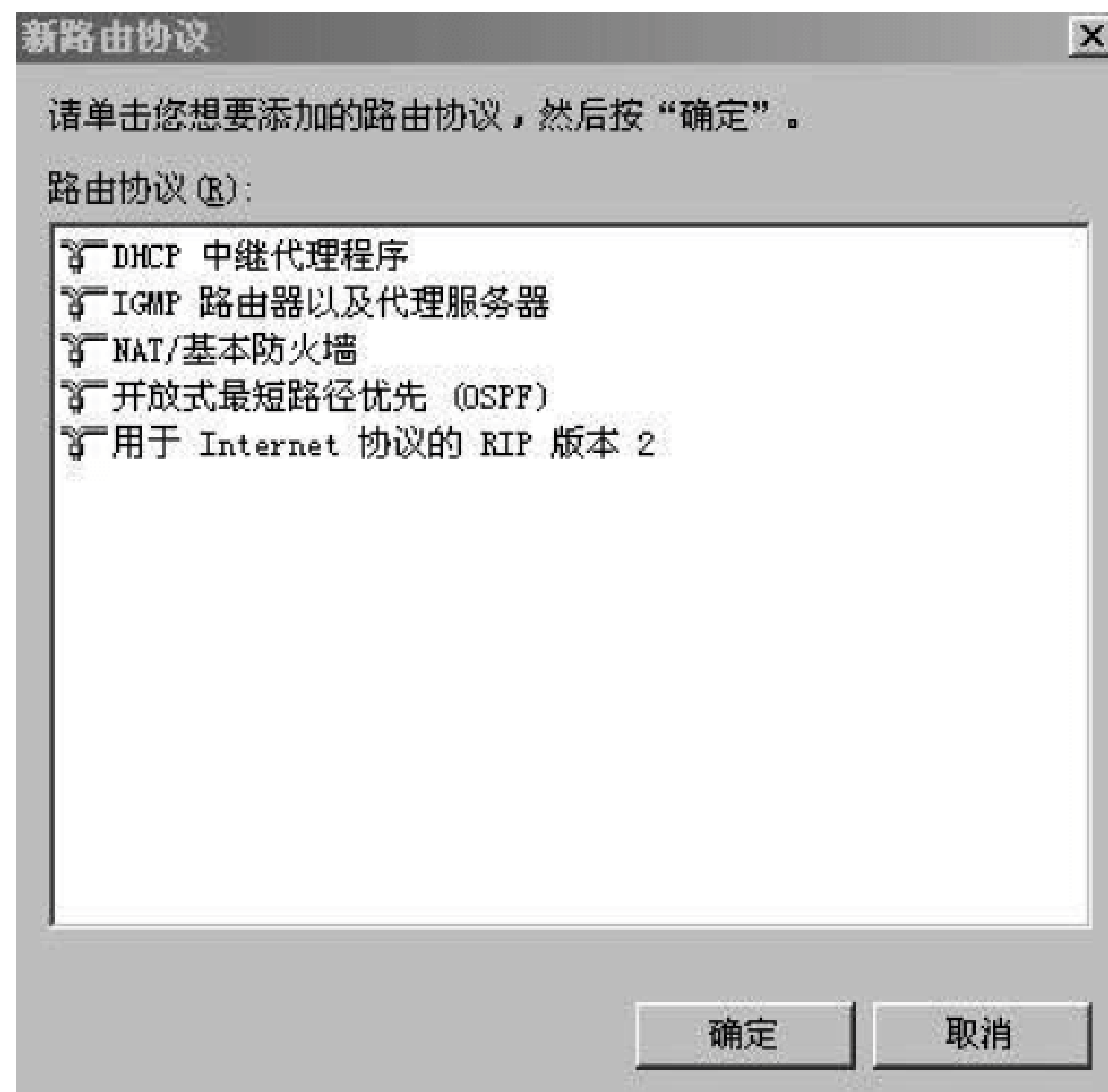



图 3-5

1. 图 3-4 中填入的 IP 地址是＿（9）＿。
2. 图 3-5 中配置 DHCP 中继代理程序，可以实现＿（10）＿。

（9）备选答案：

A. 分配给客户端的 IP 地址

B. 默认网关的 IP 地址

C. DHCP 服务器的 IP 地址

（10）备选答案：

A. 使普通客户机获取 IP 等信息

B. 跨网段的地址分配

C. 特定用户组访问特定网络

**试题三分析**

本题考查 Windows Server 2003 配置共享打印、FTP 和 DHCP 服务等相关知识。

**【问题 1】**

IPP 协议是一个基于 Internet 应用层的协议，它面向终端用户和终端打印设备。IPP

基于常用的 Web 浏览器向终端设备传送打印机的属性和状态信息需要将 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”。

Internet 打印流程如下：

① 用户输入打印设备的 URL（统一资源定位符），通过 Internet 连接到打印服务器。

② HTTP 请求通过 Internet 发送到打印服务器。

③ 打印服务器要求客户端提供身份验证信息。这样能够确保只有经过授权的用户才能在打印服务器上打印文件。

④ 当用户获得授权可以访问打印服务器后，服务器使用活动服务器页（Active Server Pages，ASP）向用户显示状态信息，其中包括有关当前空闲打印机的信息。

⑤ 当用户连接 Internet 打印网页上的任何打印机时，客户端计算机首先尝试在本地寻找该打印机的驱动程序。如果没有找到适合的驱动程序，打印服务器将会生成一个 cabinet 文件（.cab 文件，又称为 Setup 文件），其中包含正确的打印机驱动程序文件。打印服务器把 .cab 文件下载到客户端计算机上。客户端计算机提示用户允许下载该.cab 文件。

⑥ 当用户连接到 Internet 打印机后，他们可以使用 Internet 打印协议（Internet Printing Protocol，IPP）把文件发送到打印服务器。

**【问题 2】**

在 Windows Server 2003 环境下安装 FTP 服务需要在“Internet 信息服务”组件中添加“文件传输协议（FTP)”功能模块。该功能模块的配置可以实现特定用户对 FTP 的访问、建立多个 FTP 站点、显示用户连接 FTP 状态等功能。

FTP 服务器端建立的 TCP 端口号是 21。

**【问题 3】**

动态主机分配协议（DHCP）是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 Windows Server 2003 提供的组件进行 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作。在进行 DHCP 服务器配置时需要填入待分配的 IP 段以及默认网关等信息。

在大型的网络中，可能会存在多个子网。DHCP 客户机通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。如果 DHCP 客户机和服务器在不同的子网内，就要用到 DHCP 中继代理。

**参考答案**

**【问题 1】**

（1）B

（2）可采用页面显示打印机状态信息

（3）A

（4）①⑥③②⑤④

【问题 2】

（5）21

（6）在“目录安全性”页面选中“拒绝访问”，单击“添加”，在弹出的“授权访问”页面，选中“一台计算机”，填入允许访问的主机 IP

（7）增加 IP 地址或修改 TCP 端口

（8）连接 FTP 的用户或主机的信息

【问题 3】

（9）B

（10）B

**试题四（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业的网络拓扑结构如图 4-1 所示。

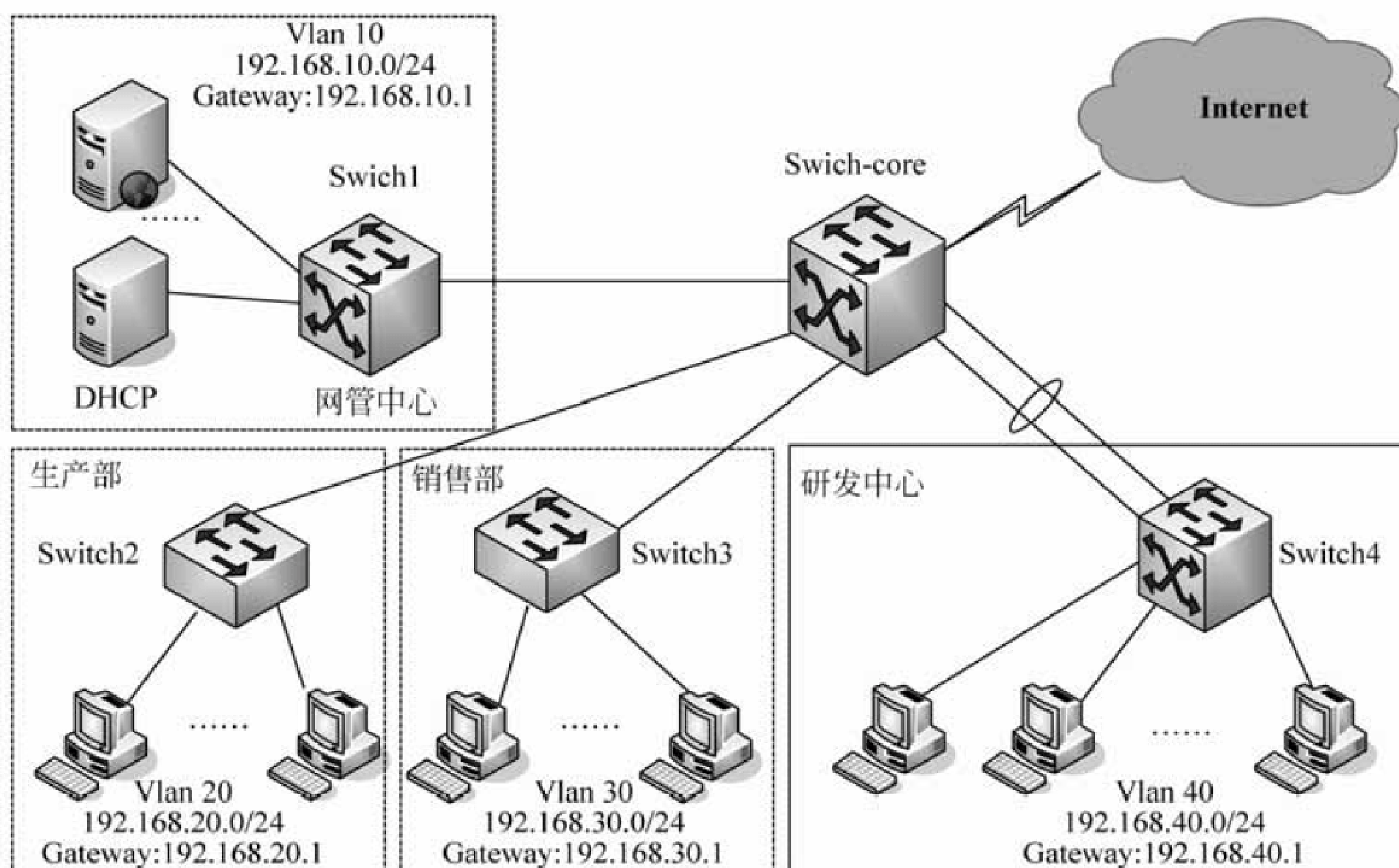



图 4-1

由于该企业路由设备数量较少，为提高路由效率，要求为该企业构建基于静态路由的多层安全交换网络。根据要求创建 4 个 VLAN 分别属于网管中心、生产部、销售部以

及研发中心，各部门的 VLAN 号及 IP 地址规划如图 4-1 所示。该企业网采用三层交换机 Switch-core 为核心交换机，Switch-core 与网管中心交换机 Switch1 和研发中心交换机 Switch4 采用三层连接，Switch-core 与生产部交换机 Switch2 及销售部交换机 Switch3 采用二层互联。

各交换机之间的连接以及接口 IP 地址如表 4-1 所示。

**表 4-1　各交换机之间的连接以及接口 IP 地址表**

| 上联端口 | | | | 下联端口 | | | |
|---|---|---|---|---|---|---|---|
| 交换机 | 端口 | 描述 | IP 地址 | 交换机 | 端口 | 描述 | IP 地址 |
| Switch-core | G0/1 | scsw-g1/1 | | Switch2 | G1/1 | core-g0/1 | |
| | G0/2 | wgsw-g0/1 | 192.168.101.1/24 | Switch1 | G0/1 | core-g0/2 | 192.168.101.2/24 |
| | F0/1 | yfsw-f0/1 | 192.168.102.1/24 | Switch4 | F0/1 | core-f0/1 | 192.168.102.2/24 |
| | F0/2 | yfsw-f0/2 | | | F0/2 | core-f0/2 | |
| | F0/3 | yfsw-f0/3 | | | F0/3 | core-f0/3 | |
| | F0/4 | yfsw-f0/4 | | | F0/4 | core-f0/4 | |
| | F0/5 | xssw-f0/1 | | Switch3 | F0/1 | core-f0/5 | |

**【问题 1】（4 分）**

随着企业网络的不断发展，研发中心的上网计算机数急剧增加，在高峰时段研发中心和核心交换机之间的网络流量非常大，在不对网络进行大的升级改造的前提下，网管人员采用了以太信道（或端口聚合）技术来增加带宽，同时也起到了＿（1）＿和＿（2）＿的作用，保证了研发中心网络的稳定性和安全性。

在两台交换机之间是否形成以太信道，可以用协议自动协商。目前有两种协商协议：一种是＿（3）＿，是 Cisco 私有的协议；另一种是＿（4）＿，是基于 IEEE 802.3ad 标准的协议。

（3）、（4）备选答案：

A．端口聚合协议（PAgP）

B．多生成树协议（MSTP）

C．链路聚合控制协议（LACP）

**【问题 2】（7 分）**

核心交换机 Switch-core 与网管中心交换机 Switch1 通过静态路由进行连接。根据需求，完成或解释 Switch-core 与 Switch1 的部分配置命令。

（1）配置核心交换机 Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
```

```
Switch-core(config-if)#description wgsw-g0/1      //___(5)___
Switch-core(config-if)#no switchport             //___(6)___
Switch-core(config-if)#ip address___(7)___
Switch-core(config-if)#no shutdown
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
Switch-core(config)#exit
…
```

（2）配置网管中心交换机 Switch1

```
Switch1#config terminal
Switch1(config)#no ip domain lookup                  //___(8)___
Switch1(config)#interface gigabitEthernet 0/1
Switch1(config-if)#description core-g0/2
Switch1(config-if)#no switchport
Switch1(config-if)#ip address___(9)___
Switch1(config-if)#exit
Switch1(config)#vlan 10
Switch1(config-vlan)#name wg10
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10                    //创建 VLAN10
Switch1(config-if)#ip address___(10)___
Switch1(config-if)#exit
Switch1(config)#interface range f0/2-20
Switch1(config-if-range)#switchport mode access      //设置端口模式为 access
                                                       模式
Switch1(config-if-range)#switchport access ___(11)___ //设置端口所属的 VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
…
```

**【问题 3】（7 分）**

为确保研发中心网络的稳定性，在现有条件下尽量保证带宽，要求实现核心交换机 Switch-core 与研发中心交换机 Switch4 的三层端口聚合，然后通过静态路由进行连接。根据需求，完成或解释以下配置命令。

（1）继续配置核心交换机 Switch-core

```
Switch-core#config terminal
```

```
Switch-core(config)#interface port-channel 10          // (12)
Switch-core(config-if)#no switchport
Switch-core(config-if)#ip address  (13)
Switch-core(config-if)#no shutdown
Switch-core(config-if)#exit
Switch-core(config)#interface range fastEthernet0/1-4   //选择配置的物理接口
Switch-core(config-if-range)#no switchport
Switch-core(config-if-range)#no ip address   //确保该物理接口没有指定的IP地址
Switch-core(config-if-range)#switchport   //改变该端口为2层接口
Switch-core(config-if-range)#channel-group 10 mode on    // (14)
Switch-core(config-if-range)#no shutdown
Switch-core(config-if-range)#exit
Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2
…
```

（2）配置研发中心交换机 Switch4

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
Switch4(config-if)#no switchport
Switch4(config-if)#ip address  (15)
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4   //选择配置的物理接口
Switch4(config-if-range)#no switchport
Switch4(config-if-range)#no ip address
…
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)# (16)                         //配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yf10
Switch4(config-vlan)#exit
Switch4(config)# (17)                 //开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
```

```
Switch4(config-if-range)#switchport mode access
…
Switch4(config-if-range)#__(18)__          //退回到特权模式
Switch4#
…
```

**【问题 4】（2 分）**

为了保障局域网用户的网络安全，防范欺骗攻击，以生产部交换机 Switch2 为例，配置 DHCP 侦听。根据需求完成或解释 Switch2 的部分配置命令。

```
Switch2#config terminal
Switch2(config)#ip dhcp snooping          //__(19)__
Switch2(config)#ip dhcp snooping vlan 20
Switch2(config)#interface gigabitEthernet1/1
Switch2(config-if)#ip dhcp snooping trust    //__(20)__
Switch2(config-if)#exit
…
```

**试题四分析**

本题考查使用三层交换机实现 VLAN 间路由的相关知识点和配置命令。

**【问题 1】**

本问题主要考查以太信道（或端口聚合）技术。

EtherChannel 是由 Cisco 研发的，应用于交换机之间的多链路捆绑技术。它的基本原理是：将两个设备间多条相同特性的快速以太或千兆位以太物理链路捆绑在一起组成一条逻辑链路，从而达到带宽倍增的目的。除了增加带宽外，EtherChannel 还可以在多条链路上均衡分配流量，起到负载均衡的作用；当一条或多条链路故障时，只要还有链路正常，流量将转移到其他的链路上，整个过程在几毫秒内完成，从而起到链路冗余的作用，增强了网络的稳定性和安全性。在 EtherChannel 中，负载在各个链路上的分布可以根据源 IP 地址、目的 IP 地址、源 MAC 地址、目的 MAC 地址、源 IP 地址和目的 IP 地址组合，以及源 MAC 地址和目的 MAC 地址组合等来进行分布。

两台交换机之间是否形成 EtherChannel 也可以用协议自动协商。目前有两个协商协议：PAgP 和 LACP，PAgP（端口汇聚协议 Port Aggregation Protocol）是 Cisco 私有的协议，而 LACP（链路汇聚控制协议 Link Aggregation Control Protocol）是基于 IEEE 802.3ad 的国际标准。语法为：channel-group [num] mode [auto | on | desirable]

其中，auto：被动协商；on：不协商；desirable：主动协商。

on 只能和 on 起 channel，两个 auto 不能起 channel。

**【问题 2】**

本问题主要考查三层交换机使用静态路由进行路由选择的配置方法。

（1）配置核心交换机 Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
//进入核心交换机三层网络接口
Switch-core(config-if)#description wgsw-g0/1
//描述该端口或者给该端口做备注
Switch-core(config-if)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch-core(config-if)#ip address 192.168.101.1 255.255.255.0
//配置三层网络接口的 IP 地址
Switch-core(config-if)#no shutdown
//激活接口
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
//配置核心交换机到 192.168.10.0 网段的静态路由
Switch-core(config)#exit
…
```

（2）配置网管中心交换机 Switch1

```
Switch1#config terminal
Switch1(config)#no ip domain lookup
//关闭域名解析功能
Switch1(config)#interface gigabitEthernet 0/1
//进入 gigabitEthernet 0/1 接口
Switch1(config-if)#description core-g0/2
//描述该接口
Switch1(config-if)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch1(config-if)#ip address 192.168.101.2 255.255.255.0
//配置三层网络接口的 IP 地址和子网掩码
Switch1(config-if)#exit
Switch1(config)#vlan 10
Switch1(config-vlan)#name wg10
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10
//进入 VLAN10 接口
```

```
Switch1(config-if)#ip address 192.168.10.1 255.255.255.0
//配置该接口的 IP 地址和子网掩码
Switch1(config-if)#exit
Switch1(config)#interface range f0/2-20
//选择接口范围为 f0/2-20
Switch1(config-if-range)#switchport mode access
//设置端口模式为 access 模式
Switch1(config-if-range)#switchport access vlan 10
//设置端口所属的 VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
//配置 switch1 到 192.168.20.0 及 192.168.30.0 网段的静态路由
…
```

**【问题 3】**

本问题主要考查冗余链路汇聚的相关配置知识。

（1）继续配置核心交换机 Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface port-channel 10
//创建编号为 10 的 port-channel 接口
Switch-core(config-if)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch-core(config-if)#ip address 192.168.102.1 255.255.255.0
//为该接口分配 IP 地址和子网掩码
Switch-core(config-if)#no shutdown
Switch-core(config-if)#exit
Switch-core(config)#interface range fastEthernet0/1-4
//选择配置的物理接口
Switch-core(config-if-range)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch-core(config-if-range)#no ip address
//确保该物理接口没有指定的 IP 地址
Switch-core(config-if-range)#switchport
//改变该端口为 2 层接口
Switch-core(config-if-range)#channel-group 10 mode on
//分配接口并指定为 PAgP 模式
```

```
Switch-core(config-if-range)#no shutdown
Switch-core(config-if-range)#exit
Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2
//配置核心交换机到192.168.40.0网段的静态路由
…
```

（2）配置研发中心交换机 Switch4

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
//创建编号为10的port-channel接口
Switch4(config-if)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch4(config-if)#ip address 192.168.102.2 255.255.255.0
//为该接口分配IP地址和子网掩码
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4
//选择配置的物理接口范围为f0/1-4
Switch4(config-if-range)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch4(config-if-range)#no ip address
//确保该物理接口没有指定的IP地址
…
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)# ip route 0.0.0.0 0.0.0.0 192.168.102.1
//配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yf10
Switch4(config-vlan)#exit
Switch4(config)# ip routing
//开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
//进入VLAN40接口
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
//配置该接口的IP地址和子网掩码
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/5-20
```

```
//选择接口范围为 f0/5-20
Switch4(config-if-range)#switchport mode access
//设置端口模式为 access 模式
…
Switch4(config-if-range)#end 或 Ctrl+Z
//在该接口模式下使用 end 或 Ctrl+Z 可直接退回到特权模式
Switch4#
…
```

**【问题 4】**

本问题主要考查交换机利用 DHCP 探测防范欺骗攻击的相关配置知识。

```
Switch2#config terminal
Switch2(config)#ip dhcp snooping
//启用 DHCP 探测
Switch2(config)#ip dhcp snooping vlan 20
//指定要实现 DHCP 探测的 VLAN
Switch2(config)#interface gigabitEthernet1/1
Switch2(config-if)#ip dhcp snooping trust
//配置端口信任，g1/1 端口为信任端口
Switch2(config-if)#exit
…
```

## 参考答案

**【问题 1】**

（1）负载均衡

（2）链路冗余

（3）A

（4）C

**【问题 2】**

（5）描述该端口或者给该端口做备注

（6）关闭二层交换功能，启用三层路由模式

（7）192.168.101.1 255.255.255.0

（8）关闭域名解析功能

（9）192.168.101.2 255.255.255.0

（10）192.168.10.1 255.255.255.0

（11）vlan 10

**【问题 3】**

（12）创建编号为 10 的 port-channel 接口

（13）192.168.102.1 255.255.255.0

（14）分配接口并指定 PAgP 模式

（15）192.168.102.2 255.255.255.0

（16）ip route 0.0.0.0 0.0.0.0 192.168.102.1

（17）ip routing

（18）end 或 Ctrl+Z

**【问题 4】**

（19）启用 DHCP 探测

（20）g1/1 端口为信任端口

# 第 27 章　2015 下半年网络工程师上午试题分析与解答

**试题（1）**

CPU 是在__（1）__结束时响应 DMA 请求的。

（1）A．一条指令执行　　B．一段程序

C．一个时钟周期　　D．一个总线周期

**试题（1）分析**

本题考查计算机组成基础知识。

DMA 控制器在需要的时候代替 CPU 作为总线主设备，在不受 CPU 干预的情况下，控制 I/O 设备与系统主存之间的直接数据传输。DMA 操作占用的资源是系统总线，而 CPU 并非在整个指令执行期间即指令周期内都会使用总线，故 DMA 请求的检测点设置在每个机器周期也即总线周期结束时执行，这样使得总线利用率最高。

**参考答案**

（1）D

**试题（2）**

虚拟存储体系由__（2）__两级存储器构成。

（2）A．主存 - 辅存　　B．寄存器 - Cache

C．寄存器 - 主存　　D．Cache - 主存

**试题（2）分析**

本题考查计算机组成基础知识。

计算机中不同容量、不同速度、不同访问形式、不同用途的各种存储器形成的是一种层次结构的存储系统。所有的存储器设备按照一定的层次逻辑关系通过软硬件连接起来，并进行有效的管理，就形成了存储体系。不同层次上的存储器发挥着不同的作用。一般计算机系统中主要有两种存储体系：Cache 存储体系由 Cache 和主存储器构成，主要目的是提高存储器速度，对系统程序员以上均透明；虚拟存储体系由主存储器和在线磁盘存储器等辅存构成，主要目的是扩大存储器容量，对应用程序员透明。

**参考答案**

（2）A

**试题（3）**

在机器指令的地址字段中，直接指出操作数本身的寻址方式称为__（3）__。

（3）A．隐含寻址　　B．寄存器寻址　　C．立即寻址　　D．直接寻址

**试题（3）分析**

本题考查计算机组成基础知识。

随着主存增加，指令本身很难保证直接反映操作数的值或其地址，必须通过某种映射方式实现对所需操作数的获取。指令系统中将这种映射方式称为寻址方式，即指令按什么方式寻找（或访问）到所需的操作数或信息（例如转移地址信息等）。可以被指令访问到的数据和信息包括通用寄存器、主存、堆栈及外设端口寄存器等。

指令中地址码字段直接给出操作数本身，而不是其访存地址，不需要访问任何地址的寻址方式被称为立即寻址。

**参考答案**

（3）C

**试题（4）**

内存按字节编址从 B3000H 到 DABFFH 的区域其存储容量为__（4）__。

（4）A．123kb　　B．159kb　　C．163kb　　D．194kb

**试题（4）分析**

本题考查计算机组成基础知识。

直接计算 16 进制地址包含的存储单元个数即可。

DABFFH – B3000H + 1 = 27C00H = 162816 = 159k，按字节编址，故此区域的存储容量为 159kb。

**参考答案**

（4）B

**试题（5）**

在软件项目管理中，以下关于人员管理的叙述，正确的是__（5）__。

（5）A．项目组成员的工作风格也应该作为组织团队时要考虑的一个要素

B．鼓励团队的每个成员充分地参与开发过程的所有阶段

C．仅根据开发人员的能力来组织开发团队

D．若项目进度滞后于计划，则增加开发人员一定可以加快开发进度

**试题（5）分析**

本题考查软件项目管理的基础知识。

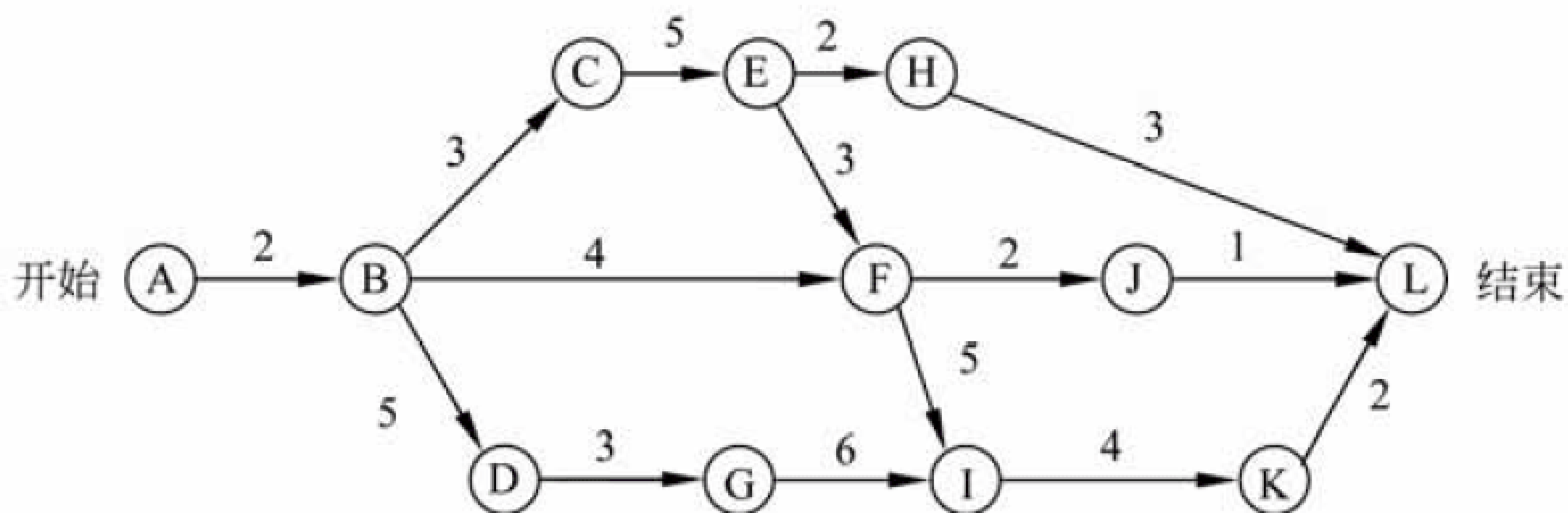
人员管理是软件项目管理的一个重要部分，在组织开发团队时，应该考虑开发人员的工作能力、知识背景、工作风格、兴趣爱好等多方面的因素。每个成员的工作任务分配清楚，不应该参与所有阶段的工作。当项目进度滞后于项目计划时，增加开发人员不一定可以加快开发进度。

**参考答案**

（5）A

**试题（6）、（7）**

某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示该活动所需的天数，则完成该项目的最少时间为 __(6)__ 天。活动 BD 最多可以晚 __(7)__ 天开始而不会影响整个项目的进度。




（6）A．9　　B．15　　C．22　　D．24

（7）A．2　　B．3　　C．5　　D．9

**试题（6）、（7）分析**

本题考查软件项目管理的基础知识。

根据上图计算出关键路径为 A→B→C→E→F→I→K→L，其长度为 24，关键路径上的活动均为关键活动。活动 BD 不在关键路径上，包含该活动的最长路径为 A→B→D→G→I→K→L，其长度为 22，因此松弛时间为 2。

**参考答案**

（6）D　（7）A

**试题（8）、（9）**

在 Windows 系统中，设 E 盘的根目录下存在 document1 文件夹，用户在该文件夹下已创建了 document2 文件夹，而当前文件夹为 document1。若用户将 test.docx 文件存放在 document2 文件夹中，则该文件的绝对路径为 __(8)__；在程序中能正确访问该文件且效率较高的方式为 __(9)__。

（8）A．\document1\　　B．E:\document1\ document2

C．document2\　　D．E:\document2\document1

（9）A．\document1\ test.docx　　B．document1\ document2\test.docx

C．document2\test.docx　　D．E:\document1\document2\test.docx

**试题（8）、（9）分析**

按查找文件的起点不同可以将路径分为：绝对路径和相对路径。从根目录开始的路径称为绝对路径；从用户当前工作目录开始的路径称为相对路径，相对路径是随着当前工作目录的变化而改变的。

在 Windows 操作系统中，绝对路径是从根目录开始到文件所经过的文件夹名构成的，并以“\”开始，表示根目录；文件夹名之间用符号“\”分隔。按题意，“test.docx”

的绝对路径表示为：E:\document1\document2。相对路径是从当前文件夹开始到文件所经过的文件夹名。编程时采用相对路径名 document2\test.docx，不仅能正确地访问该文件而且效率也更高。

**参考答案**

（8）B （9）C

**试题（10）**

软件设计师王某在其公司的某一综合信息管理系统软件开发工作中承担了大部分程序设计工作。该系统交付用户，投入试运行后，王某辞职离开公司，并带走了该综合信息管理系统的源程序，拒不交还公司。王某认为，综合信息管理系统源程序是他独立完成的，他是综合信息管理系统源程序的软件著作权人。王某的行为 （10） 。

（10）A．侵犯了公司的软件著作权　　B．未侵犯公司的软件著作权
C．侵犯了公司的商业秘密权　　D．不涉及侵犯公司的软件著作权

**试题（10）分析**

王某的行为侵犯了公司的软件著作权。因为王某作为公司的职员，完成的某一综合信息管理系统软件是针对其本职工作中明确指定的开发目标而开发的软件。该软件应为职务作品，并属于特殊职务作品。公司对该软件享有除署名权外的软件著作权的其他权利，而王某只享有署名权。王某持有该软件源程序不归还公司的行为，妨碍了公司正常行使软件著作权，构成对公司软件著作权的侵犯，应承担停止侵权法律责任，交还软件源程序。

**参考答案**

（10）A

**试题（11）**

集线器与网桥的区别是 （11） 。

（11）A．集线器不能检测发送冲突，而网桥可以检测冲突
B．集线器是物理层设备，而网桥是数据链路层设备
C．网桥只有两个端口，而集线器是一种多端口网桥
D．网桥是物理层设备，而集线器是数据链路层设备

**试题（11）分析**

集线器是物理层设备，相当于在 10Base2 局域网中把连接工作站的同轴电缆收拢在一个盒子里，这个盒子只起到接收和发送的功能，可以检测发送冲突，但不能识别数据链路层的帧。网桥是数据链路层设备，它可以识别数据链路层 MAC 地址，有选择地把帧发送到输出端口，网桥也可以有多个端口，如果网桥端口很多，并配置了加快转发的硬件，就成为局域网交换机。

**参考答案**

（11）B

**试题（12）、（13）**

根据 STP 协议，网桥 ID 最小的交换机被选举为根网桥，网桥 ID 由＿（12）＿字节的优先级和 6 字节的＿（13）＿组成。

（12）A．2　　B．4　　C．6　　D．8

（13）A．用户标识　　B．MAC 地址　　C．IP 地址　　D．端口号

**试题（12）、（13）分析**

根据 STP 协议，网桥 ID 由 2 字节的网桥优先级和 6 字节的网桥MAC 地址组成，取值范围为 0～65535，默认值为 32768。

**参考答案**

（12）A　（13）B

**试题（14）**

关于 ICMP 协议，下面的论述中正确的是＿（14）＿。

（14）A．通过 ICMP 可以找到与 MAC 地址对应的 IP 地址

B．通过 ICMP 可以把全局 IP 地址转换为本地 IP 地址

C．ICMP 用于动态分配 IP 地址

D．ICMP 可传送 IP 通信过程中出现的错误信息

**试题（14）分析**

ICMP 与 IP 同属于网络层协议，用于传送有关通信问题的消息，例如数据报不能到达目标，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。支持 IPv6 地址的 ICMPv6 协议增加的邻居发现功能代替了 ARP 协议，ICMPv6 还为支持 IPv6 中的路由优化、IP 组播、移动 IP 等增加了一些新的报文类型。

**参考答案**

（14）D

**试题（15）**

设信号的波特率为 500Baud，采用幅度-相位复合调制技术，由 4 种幅度和 8 种相位组成 16 种码元，则信道的数据速率为＿（15）＿。

（15）A．500 b/s　　B．1000 b/s　　C．2000 b/s　　D．4800 b/s

**试题（15）分析**

根据尼奎斯特定理，若信道带宽为 W，则最大码元速率为

$$B=2W \text{（Baud）}$$

尼奎斯特定理指定的信道容量也叫作尼奎斯特极限，这是由信道的物理特性决定的。码元携带的信息量由码元取的离散值个数决定。若码元取两个离散值，则一个码元携带 1 比特（bit）信息。若码元可取 4 种离散值，则一个码元携带 2 比特信息。总之一个码元携带的信息量 n（比特数）与码元的种类个数 N 有如下关系：

$$n=\log_2 N \quad (N=2^n)$$

单位时间内在信道上传送的信息量（比特数）称为数据速率。在一定的波特率下提高速率的途径是用一个码元表示更多的比特数。如果把 2 比特编码为一个码元，则数据速率可成倍提高，公式为

$$R=B\log_2 N=2W\log_2 N\ (\text{b/s})$$

在本题中 $B$=500Baud，$N$=16，所以 $R=B\log_2 N=500\times\log_2 16$=2000b/s

**参考答案**

（15）C

**试题（16）、（17）**

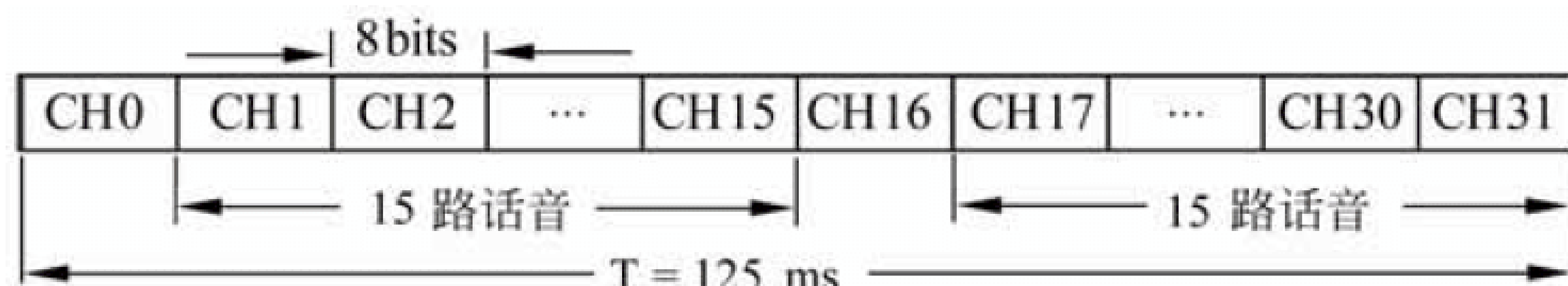
E1 载波的数据速率是＿（16）＿。E3 载波的数据速率是＿（17）＿。

（16）A．64kb/s　B．2.048Mb/s　C．34.368Mb/s　D．139.26Mb/s

（17）A．64kb/s　B．2.048Mb/s　C．34.368Mb/s　D．139.26Mb/s

**试题（16）、（17）分析**

ITU-T E1 信道的数据速率是 2.048 Mb/s（见下图）。这种载波把 32 个 8 位一组的数据样本组装成 125μs 的基本帧，其中 30 个子信道用于话音传送数据，2 个子信道（CH0 和 CH16）用于传送控制信令，每 4 帧能提供 64 个控制位。除了北美和日本外，E1 载波在其他地区得到广泛使用。




按照 ITU-T 的多路复用标准，E2 载波由 4 个 E1 载波组成，数据速率为 8.448Mb/s。E3 载波由 4 个 E2 载波组成，数据速率为 34.368 Mb/s。E4 载波由 4 个 E3 载波组成，数据速率为 139.264 Mb/s。E5 载波由 4 个 E4 载波组成，数据速率为 565.148 Mb/s。

**参考答案**

（16）B　（17）C

**试题（18）、（19）**

ADSL 采用＿（18）＿技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供电话和上网服务。采用 ADSL 联网，计算机需要通过＿（19）＿和分离器连接到电话入户接线盒。

（18）A．时分复用　B．频分复用　C．空分复用　D．码分多址

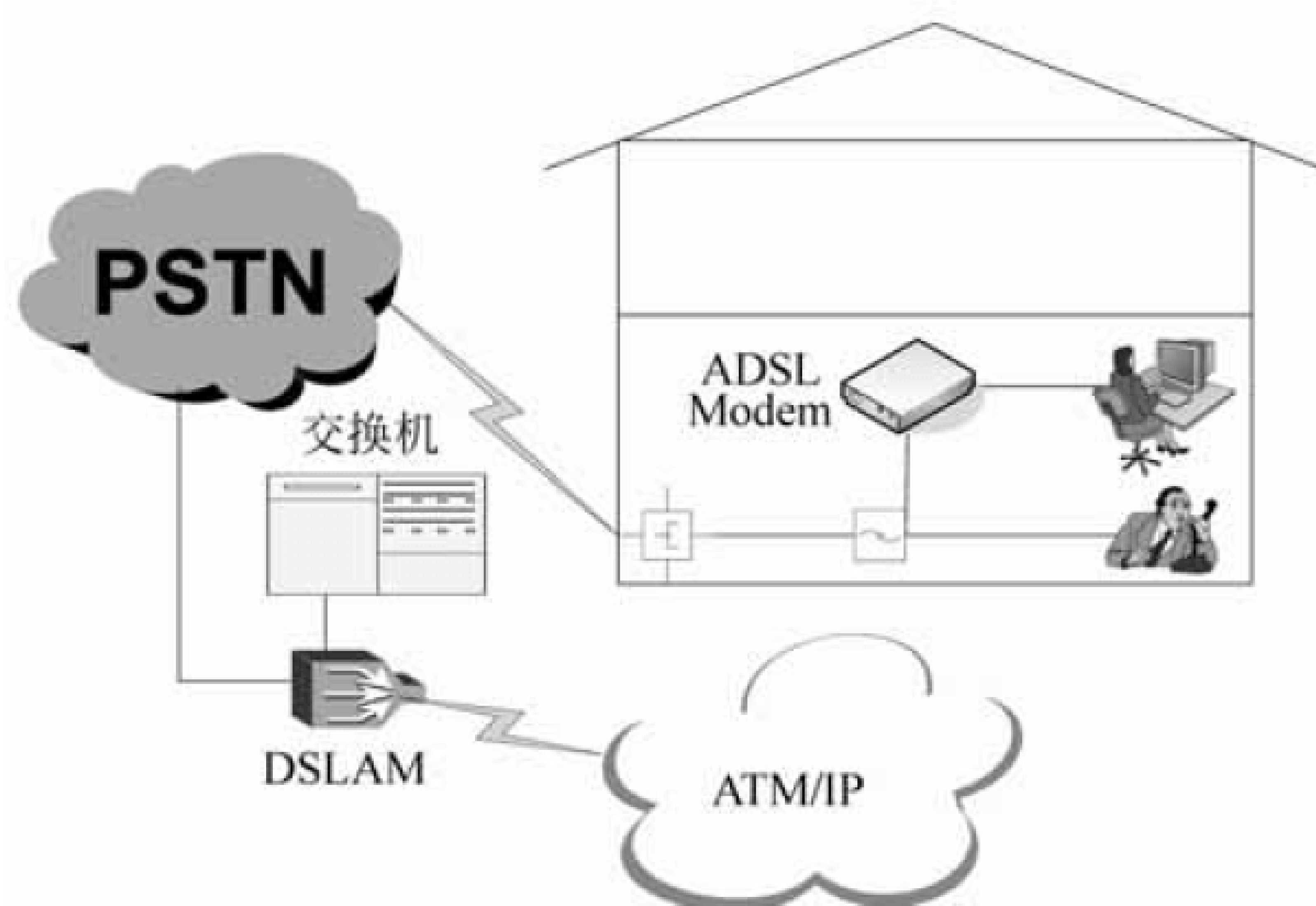
（19）A．ADSL 交换机　B．Cable Modem

　　　C．ADSL Modem　D．无线路由器

**试题（18）、（19）分析**

数字用户线路（Digital Subscriber Line，DSL）是以铜质电话线为传输介质的通信技术组合，采用频分复用技术把 PSTN 线路划分为话音、上行和下行三个独立的信道。非

对称 DSL（Asymmetric DSL，ADSL）在一对铜线上支持上行速率 640kb/s～1Mb/s、下行速率 1Mb/s～8Mb/s，有效传输距离在 3～5 公里范围以内。在提供话音服务的同时还可以满足网上冲浪和视频点播等应用对带宽的要求。采用 ADSL 联网，计算机需要通过 ADSL Modem 和分离器连接到电话入户接线盒，如下图所示。

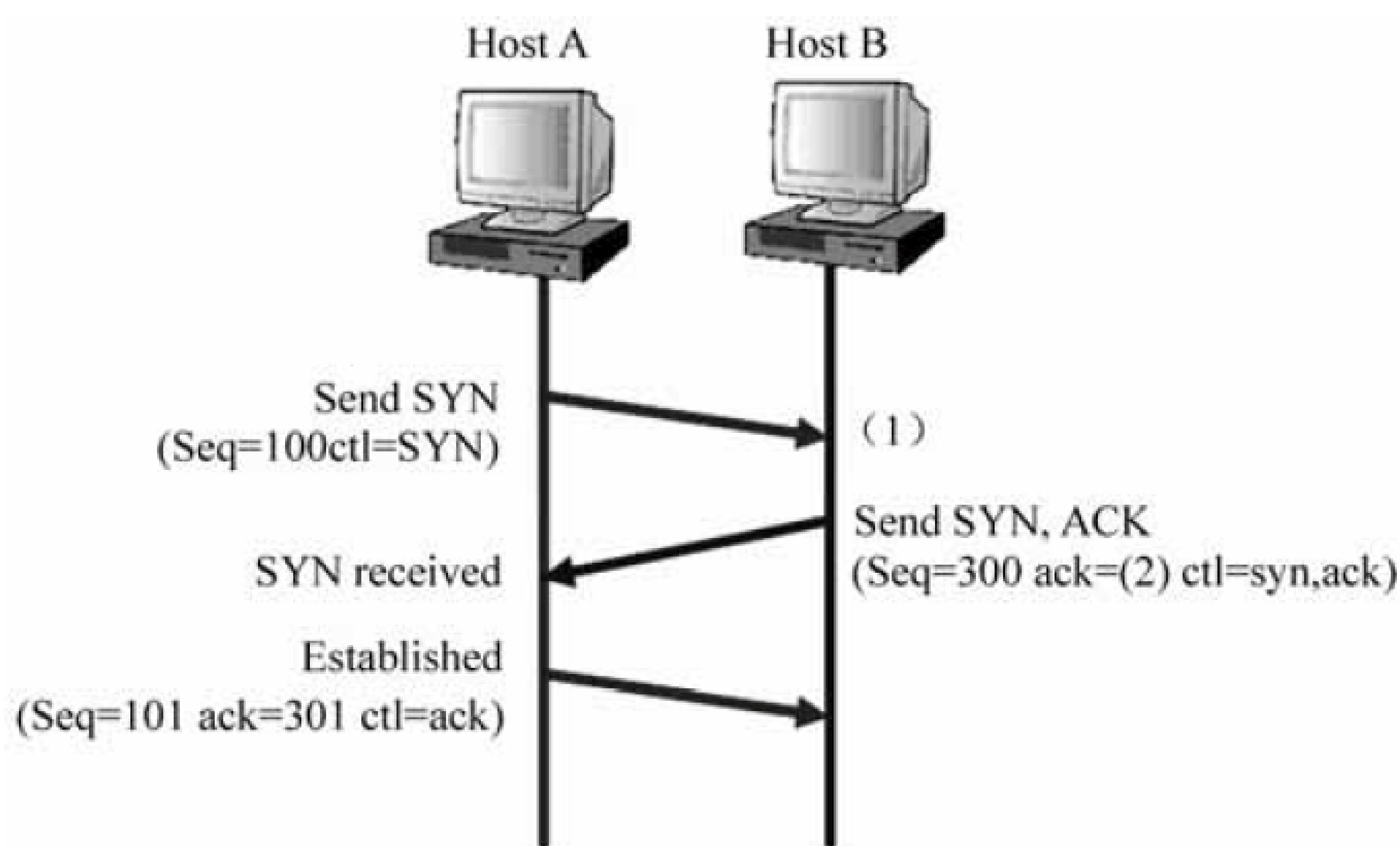



**参考答案**

（18）B　（19）C

**试题（20）、（21）**

下图中主机 A 和主机 B 通过三次握手建立 TCP 连接，图中（1）处的状态是 （20） ，（2）处的数字是 （21） 。




（20）A．SYN received　　B．Established
　　C．Listen　　D．FIN wait

（21）A．100　　B．101　　C．300　　D．301

**试题（20）、（21）分析**

TCP 连接管理如下图所示。由于主机 A 发出了连接请求（Send SYN），所以主机 B 收到这个请求时的状态是 SYN received。又由于主机 A 发出的序列号是 100，所以主机

B 准备从 101 字节开始接收。



**参考答案**

（20）A （21）B

**试题（22）**

TCP 使用的流量控制协议是__（22）__。

（22）A. 固定大小的滑动窗口协议 B. 可变大小的滑动窗口协议

C. 后退 N 帧 ARQ 协议 D. 停等协议

**试题（22）分析**

TCP 的流量控制采用了可变大小的滑动窗口协议，由接收方指明接收缓冲区的大小（字节数），发送方发送了规定的字节数后等待接收方的下一次请求。固定大小的滑动窗口协议用在数据链路层的 HDLC 中。可变大小的滑动窗口协议可以应付长距离通信过程中线路延迟不确定的情况，而固定大小的滑动窗口协议则适合链路两端点之间通信延迟固定的情况。

**参考答案**

（22）B

**试题（23）**

下面 4 种路由中，哪一种路由的子网掩码是 255.255.255.255？__（23）__。

（23）A. 远程网络路由　B. 主机路由
C. 默认路由　D. 静态路由

**试题（23）分析**

主机路由的子网掩码是 255.255.255.255。网络路由要指明一个子网，所以不可能为全 1，默认路由是访问默认网关，而默认网关与本地主机属于同一个子网，其子网掩码也应该与网络路由相同，对静态路由也是同样的道理。

**参考答案**

（23）B

**试题（24）～（26）**

边界网关协议 BGP4 是一种动态路由发现协议，它的主要功能是__（24）__。BGP 路由器之间传送的是 AS 路径信息，这样就解决了__（25）__问题。BGP4 报文封装在__（26）__中传送。

（24）A. 发现新的路由　B. 计算最短通路
C. 控制路由策略　D. 维护网络拓扑数据库

（25）A. 路由环路　B. 最短通路
C. 路由计算　D. 路由更新

（26）A. IP 数据报　B. 以太帧
C. TCP 报文　D. UDP 报文

**试题（24）～（26）分析**

外部网关协议 BGP 4 是一种动态路由发现协议，其主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 路由器之间传送的是 AS 路径信息，由一个目标网络地址后跟一串要经过的 AS 的编号组成，如果该串中出现了相同的 AS 编号，这就是出现了路由环路。

BGP4 报文封装在 TCP 报文中传送，在封装层次上看似 TCP 的上层协议，但是从功能上理解它解决的是路由问题，所以仍然属于网络层协议。

**参考答案**

（24）C　（25）A　（26）C

**试题（27）**

在广播网络中，OSPF 协议要选定一个指定路由器（DR），指定路由器的功能是__（27）__。

（27）A. 发送链路状态公告　B. 检查网络故障
C. 向其他路由器发送最新路由表　D. 发现新增加的路由器

**试题（27）分析**

OSPF 是一种链路状态协议，用于在自治内部路由器之间交换路由信息。链路状态协议是从各个路由器收集链路状态信息，构造网络拓扑结构图，使用 Dijkstra 的最短通路优先（SPF）算法计算到达各个目标的最佳路由。

如果两个路由器都通过各自的接口连接到一个共同的网络上，则它们是邻居（Neighboring）关系。路由器可以在其邻居中选择需要交换链路状态信息的路由器，与之建立毗邻关系（Adjacency）。并不是每一对邻居都需要交换路由信息，因而不是每一对邻居都要建立毗邻关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器（Designated Router，DR），其他的路由器都与 DR 建立毗邻关系，把自己掌握的链路状态信息提交给 DR，由 DR 代表这个网络向外界发布。可以看出，DR 的存在减少了毗邻关系的数量，从而也减少了向外发布的路由信息量。

OSPF 路由器之间通过链路状态公告（Link State Advertisment，LSA）交换网络拓扑信息。LSA 中包含连接的接口、链路的度量值（Metric）等信息。

**参考答案**

（27）A

**试题（28）、（29）**

POP3 协议采用__（28）__模式，客户端代理与 POP3 服务器通过建立__（29）__连接来传送数据。

（28）A．Browser/Server　　B．Client/Server
　　C．Peer to Peer　　D．Peer to Server

（29）A．TCP　　B．UDP　　C．P2P　　D．IP

**试题（28）、（29）分析**

本题考查 POP3 协议及 POP3 服务器方面的基础知识。

POP3 协议是 TCP/IP 协议簇中用于邮件接收的协议。邮件客户端通过与服务器之间建立 TCP 连接，采用 Client/Server 计算模式来传送邮件。

**参考答案**

（28）B　（29）A

**试题（30）**

如果要将目标网络为 202.117.112.0/24 的分组经 102.217.115.1 接口发出，需增加一条静态路由，正确的命令为__（30）__。

（30）A．route add 202.117.112.0　255.255.255.0　102.217.115.1
　　B．route add 202.117.112.0　0.0.0.255　102.217.115.1
　　C．add route 202.117.112.0　255.255.255.0　102.217.115.1
　　D．add route 202.117.112.0　0.0.0.255　102.217.115.1

**试题（30）分析**

本题考查路由配置命令格式方面的基础知识。

route 命令的功能是显示和修改本地的 IP 路由表，语法如下：

route [-f] [-p] [*Command* [*Destination*] [mask *Netmask*] [*Gateway*] [metric *Metric*]] [if *Interface*]]

Command 命令值为 add，表示添加路由。目标网络为 202.117.112.0/24，且接口为 102.217.115.1 ，故正确的命令为：

route　add　202.117.112.0　255.255.255.0　102.217.115.1

**参考答案**

（30）A

**试题（31）**

在 Linux 系统中，使用 ifconfig 设置接口的 IP 地址并启动该接口的命令是__（31）__。

（31）A．ifconfig eth0 192.168.1.1 mask 255.255.255.0

B．ifconfig 192.168.1.1 mask 255.255.255.0 up

C．ifconfig eth0 192.168.1.1 mask 255.255.255.0 up

D．ifconfig 192.168.1.1 255.255.255.0

**试题（31）分析**

本题目考查是在 Linux 系统下基本命令使用的基础知识。

在 Linux 系统下，设置接口 IP 地址，并将接口启动的命令格式是：

ifconfig　接口名称　IP 地址　mask　子网掩码　up/down

根据以上命令格式，据题意可知，C 为正确答案。

**参考答案**

（31）C

**试题（32）**

在 Linux 系统中，可通过__（32）__文件查看一台主机的名称和完整域名。

（32）A．etc/dev　　B．etc/conf　　C．etc/hostname　　D．etc/network

**试题（32）分析**

本题目考查是在 Linux 系统文件系统的基础知识。

在 Linux 操作系统中，TCP/IP 网络是通过若干个文本文件进行配置的。系统在启动时通过读取一组有关网络配置的文件和脚本参数内容，来实现网络接口的初始化和控制过程，这些文件和脚本大多数位于/etc 目录下。

/etc/hostname 文件包含了 Linux 系统的主机名称，包括完全的域名。

/etc/host.conf 文件指定如何解析主机域名，Linux 通过解析器库来获得主机名对应的 IP 地址。

/etc/sysconfig/network 是一个用来指定服务器上的网络配置信息的文件，包含了控制

和网络有关的文件和守护程序行为的参数。

**参考答案**

（32）C

**试题（33）、（34）**

在 Windows 客户端运行 nslookup 命令，结果如下图所示。为 www.softwaretest.com 提供解析的是＿（33）＿。在 DNS 服务器中，ftp．softwaretest.com 记录通过＿（34）＿方式建立。

```
C:\Documents and Settings\user>nslookup  www.softwaretest.com
Server:    ns1.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:     www.softwaretest.com
Address: 10.10.1.3

C:\Documents and Settings\user>nslookup  ftp.softwaretest.com
Server:    ns1.softwaretest.com
Address: 192.168.1.254

Non-authoritative answer:
Name:     ns1.softwaretest.com
Address:  10.10.1.1
Aliases:  ftp.softwaretest.com
```

（33）A．192.168．1.254　　B．10.10.1.3
　　C．10.10.1.1　　D．192.168．1.1

（34）A．主机　　B．别名　　C．邮件交换器　　D. PTR 记录

**试题（33）、（34）分析**

本题考查 DNS 服务器方面的基础知识。

nslookup 命令显示的是为域名提供解析的服务器及相关资源记录。记录显示为 www. softwaretest.com 及 ftp. Softwaretest.com，提供解析的服务器是 ns1.softwaretest.com，其 IP 地址为 192.168.1.254。

又由记录显示 ftp.softwaretest.com 是 10.10.1.1 主机上通过别名建立的域名。

**参考答案**

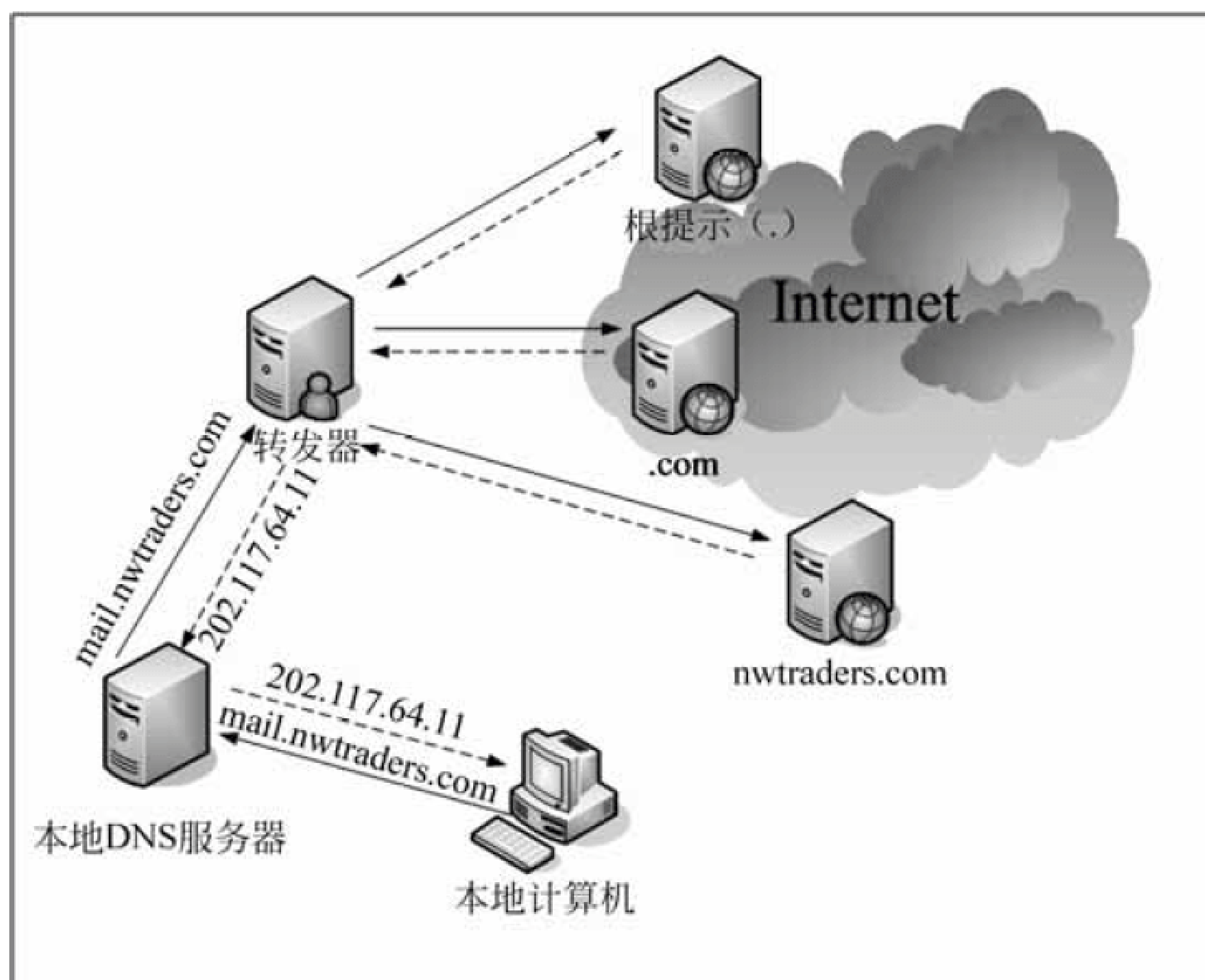
（33）A　（34）B

**试题（35）**

下图是 DNS 转发器工作的过程。采用迭代查询算法的是＿（35）＿。

（35）A．转发器和本地 DNS 服务器
　　B．根域名服务器和本地 DNS 服务器
　　C．本地 DNS 服务器和.com 域名服务器

D．根域名服务器和.com 域名服务器




**试题（35）分析**

本题考查 DNS 服务器递归算法和迭代算法方面的基础知识。

递归查询只发出一次查询请求，要求服务器彻底地进行名字解析。当需要进一步查询时，本域名服务器向上级域名服务器返回其他域名服务器发出请求，直到查到记录。

迭代查询可能发出多条请求，即上级域名服务器若返回的是其他域名服务器的地址，本域名服务器把这个地址发给用户，用户再进行深一级的查询。

从本题中可以看出，根域名服务器发回给转发器的是.com 服务器地址，并不是结果，故采用的是迭代算法；.com 域名服务器发回给转发器的是授权域名服务器 nwtraders.com 服务器地址，也不是结果，采用的也是迭代算法；nwtraders.com 服务器尽管返回给转发器域名和 IP 的对应关系，但它是授权域名服务器，在其资源记录中已经找到了记录，故其采用的算法未知。本地域名服务器只向转发器发出了 1 条请求，转发器经过多次深层次查询，返回的是查到的记录，故转发器采用的是递归算法。本地域名服务器采用的算法未知。

**参考答案**

（35）D

**试题（36）**

下列域名中，格式正确的是__（36）__。

（36）A．-123456.com　　B．123-456.com

C．123*456.com　　D．123456-.com

**试题（36）分析**

本题目考查域名的基础知识。

一个合法的域名可以由字母、数字、下划线构成，不能存在除以上三种字符之外的其他字符，并且不能以下划线开始和结束。

**参考答案**

（36）B

**试题（37）**

以下关于域名查询的叙述中，正确的是＿（37）＿。

（37）A．正向查询是检查 A 记录，将 IP 地址解析为主机名

B．正向查询是检查 PTR 记录，将主机名解析为 IP 地址

C．反向查询是检查 A 记录，将主机名解析为 IP 地址

D．反向查询是检查 PTR 记录，将 IP 地址解析为主机名

**试题（37）分析**

本题考查域名解析的基础知识。

DNS 中的 A (Address) 记录用来指定主机名（或域名）对应的 IP 地址记录。

DNS 中的 PTR 记录是用来指定 IP 地址对应的主机名（或域名）记录。

在 DNS 查询中，有正向查找和反向查找两种，其中，正向查找是利用查询 A 记录，根据域名来查找与之对应的 IP 地址的过程；反向查找是查找 PTR 记录，根据 IP 地址来查找与之对应的主机名（或域名）的过程。

**参考答案**

（37）D

**试题（38）**

下列地址中，＿（38）＿不是 DHCP 服务器分配的 IP 地址。

（38）A．196.254.109.100　　B．169.254.109.100

C．96.254.109.100　　D．69.254.109.100

**试题（38）分析**

本题考查 DHCP 的基础知识。

DHCP 是用于自动为客户端分配 IP 地址的一种服务器，当客户端向服务器端申请 IP 地址时，首先发送 DHCP Discovery 消息，用来查找范围内的 DHCP 服务器，如果客户端找到了合法的 DHCP 服务器，服务器会向该客户端发送一个合法的 IP 地址。如果经过查找，并未找到任何 DHCP 服务器，这时，系统会自动为客户端分配一个 IP 地址，在 Windows 系统下，分配的地址是 169.254.0.0 段的任何一个地址。因此，169.254.0.0 段的地址不会是由 DHCP 服务器分配给客户端的地址。

**参考答案**

（38）B

**试题（39）、（40）**

下图是配置某邮件客户端的界面，图中 a 处应填写__（39）__，b 处应填写__（40）__。

（39）A. abc.com　　B. POP3.abc.com

C. POP.com　　D. POP3.com

（40）A. 25　　B. 52　　C. 100　　D. 110

**试题（39）、（40）分析**

本题考查邮件客户端设置的基础知识。

在设置邮件客户端程序时，需设置相应的发送邮件服务器（SMTP 服务器）和接收邮件服务器（POP 服务器）。根据题意，邮件发送使用 SMTP 协议，因此服务器的地址是 SMTP.abc.com，其对应端口是 25 号端口；接收邮件使用 POP3 服务器，服务器的地址是 POP3.abc.com，对应端口是 110。

**参考答案**

（39）B　（40）D

**试题（41）**

__（41）__不属于主动攻击。

（41）A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

**试题（41）分析**

本题考查网络攻击的基础知识。

网络攻击有主动攻击和被动攻击两类。其中主动攻击是指通过一系列的方法，主动地向被攻击对象实施破坏的一种攻击方式，例如重放攻击、IP 地址欺骗、拒绝服务攻击等均属于攻击者主动向攻击对象发起破坏性攻击的方式。流量分析攻击是通过持续检测现有网络中的流量变化或者变化趋势，而得到相应信息的一种被动攻击方式。

**参考答案**

（41）A

**试题（42）、（43）**

下列算法中，可用于报文认证的是__（42）__，可以提供数字签名的是__（43）__。

（42）A．RSA　B．IDEA　C．RC4　D．MD5

（43）A．RSA　B．IDEA　C．RC4　D．MD5

**试题（42）、（43）分析**

本题考查报文认证和数字签名的基础知识。

报文认证是指在网络上对接收到的报文的完整性进行确认的过程。一般实现时使用一种散列函数，例如 MD5 或者 SHA-1，将任意长度的文本作为输入，产生长度为 L 的输出，作为报文认证信息与原报文一同发送给接收者，接收者接收到文本后，使用相同的散列函数进行计算，将计算结果与报文认证信息进行对比之后即可验证文本的完整性和真实性。而数字签名是使用公钥体制（如 RSA）产生的一对公钥和私钥，使用私钥对报文进行签名，使用公钥对文件的签名进行验证，起到保证文件的不可否认性的作用。

**参考答案**

（42）D　（43）A

**试题（44）**

下列__（44）__不能提供应用层安全。

（44）A．S-HTTP　B．PGP　C．MIME　D．SET

**试题（44）分析**

本题考查应用层安全协议的基础知识。

以上 4 个选项中，S-HTTP 是传输经过 SSL 加密的超文本信息的协议，一般用于安全性要求较高的 Web 浏览环境，如电子商务网页浏览、通过网页支付等环境，它提供的是应用层的安全服务。

PGP 是传输安全电子邮件的协议，可对电子邮件进行加密、签名等操作，它提供的是应用层安全服务。

MIME（Multipurpose Internet Mail Extensions，多用途互联网邮件扩展类型）是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。它并未提供任何应用层安全服务。

SET（Secure Electronic Transaction，简称 SET 协议）主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份，以及可操作性。SET 中的核心技术主要有公开密钥加密、数字签名、电子信封、安全证书等，它提供的是应用层安全服务。

**参考答案**

（44）C

**试题（45）**

防火墙不具备__（45）__功能。

（45）A．包过滤　B．查毒　C．记录访问过程　D．代理

**试题（45）分析**

本题考查防火墙基础知识。

防火墙是一种放置在网络边界上，用于保护内部网络安全的网络设备。它通过对流经的数据流进行分析和检查，可实现对数据包的过滤、保存用户访问网络的记录和服务器代理功能。防火墙不具备检查病毒的功能。

**参考答案**

（45）B

**试题（46）**

如下图所示，从输出的信息中可以确定的是__（46）__。

```
C:\> netstat -n

Active Connections

  Proto   Local Address          Foreign Address       State
  TCP     192.168.0.200:2011     202.100.112.12:443    ESTABLISHED
  TCP     192.168.0.200:2038     100.29.200.110:110    TIME_WAIT
  TCP     192.168.0.200:2052     128.105.129.30:80     ESTABLISHED
```

（46）A．本地主机正在使用的端口号是公共端口号

B．192.168.0.200 正在与 128.105.129.30 建立连接

C．本地主机与 202.100.112.12 建立了安全连接

D．本地主机正在与 100.29.200.110 建立连接

**试题（46）分析**

本题考查网管命令 netstat -n 的含义。

从 netstat -n 的输出信息中可以看出，本地主机 192.168.0.200 使用的端口号 2011、2038、2052 都不是公共端口号。根据状态提示信息，其中已经与主机 128.105.129.30 建立了连接，与主机 100.29.200.110 正在等待建立连接，与主机 202.100.112.12 已经建立了安全连接。

**参考答案**

（46）C

**试题（47）**

为防止 WWW 服务器与浏览器之间传输的信息被窃听，可以采取__（47）__来防止该事件的发生。

（47）A．禁止浏览器运行 Active X 控件
B．索取 WWW 服务器的 CA 证书
C．将 WWW 服务器地址放入浏览器的可信站点区域
D．使用 SSL 对传输的信息进行加密

**试题（47）分析**

本题考查利用 SSL 传输的相关知识。

SSL 是一个安全协议，它提供使用 TCP/IP 的通信应用程序间的隐私与完整性。因特网的超文本传输协议（HTTP）使用 SSL 来实现安全的通信。

SSL 协议位于 TCP 协议与各种应用层协议之间，为数据通讯提供安全支持。SSL 协议可分为两层。SSL 记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 SSL 握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。提供的服务如下：

① 认证用户和服务器，确保数据发送到正确的客户机和服务器；
② 加密数据以防止数据中途被窃取；
③ 维护数据的完整性，确保数据在传输过程中不被改变。

**参考答案**

（47）D

**试题（48）**

某用户无法访问域名为 www.cisco.com 的网站，在用户主机上执行 tracert 命令得到提示如下：

```
Tracing route to www.cisco.com[119.188.155.27]
Over amaximum of 30 hops:
1  <1ms   <1ms   <1ms    202.117.112.129
2  202.117.112.129   reports:Destination net unreachable
```

根据提示信息，造成这种现象的原因可能是__（48）__。

（48）A．用户主机的网关设置错误
B．用户主机设置的 DNS 服务器工作不正常
C．路由器上进行了相关 ACL 设置
D．用户主机的 IP 地址设置错误

**试题（48）分析**

本题考查网管命令 tracert 的含义。

从 tracert 的输出信息中可以看出，DNS 解析正常，说明 DNS 服务器工作正常；第一跳到网关<1ms，说明网关设置正确；那么说明用户主机的 IP 地址设置也没有问题，由网关给出目标不可达信息，说明可能在路由器上进行了相关 ACL 设置，不允许访问。

**参考答案**

（48）C

**试题（49）**

下列网络管理软件中不需要 SNMP 支持的是__（49）__。

（49）A．CiscoWorks　B．Netview　C．Solarwinds　D．Wireshark

**试题（49）分析**

本题考查网管命令网络管理软件的使用常识。

在这 4 个软件中，CiscoWorks、Netview 以及 Solarwinds 都是网络管理软件，都必须得到 SNMP 的支持，而 Wireshark（前称 Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料，并不要求 SNMP 的支持。

**参考答案**

（49）D

**试题（50）**

在 SNMPv2 错误类型中，表示管理对象不可访问的是__（50）__。

（50）A．noAccess　B．genErr　C．wrongValue　D．noCreation

**试题（50）分析**

本题考查 SNMPv2 的错误类型。

在 SNMPv2 错误类型中，表示管理对象不可访问的是 noAccess。而 genErr 表示某些其他的差错。若代理不执行该操作，则返回 wrongValue。noCreation 则表示对象不存在且无法建立。

**参考答案**

（50）A

**试题（51）**

通过 CIDR 技术，把 4 个主机地址 220.78.169.5、220.78.172.10、220.78.174.15 和 220.78.168.254 组织成一个地址块，则这个超级地址块的地址是__（51）__。

（51）A．220.78.177.0/21　B．220.78.168.0/21

C．220.78.169.0/20　D．220.78.175.0/20

**试题（51）分析**

地址 220.78.169.5 的二进制表示是：　1101 1100.0100 1110.1010 1001.0000 0101

地址 220.78.172.10 的二进制表示是：　1101 1100.0100 1110.1010 1100.0000 1010

地址 220.78.174.15 的二进制表示是：　1101 1100.0100 1110.1010 1110.0000 1111

地址 220.78.168.254 的二进制表示是：　1101 1100.0100 1110.1010 1000.1111 1110

4 个地址共同的部分是　1101 1100.0100 1110.1010 1

所以取 220.78.168.0/21 作为超级地址块。**1101 1100.0100 1110.1010 1**000.0000 0000

**参考答案**

（51）B

**试题（52）**

采用可变长子网掩码可以把大的网络分成小的子网，例如把 A 类网络 60.15.0.0/16 分为两个子网，假设第一个子网为 60.15.0.0/17，则另一个子网为__（52）__。

（52）A．60.15.1.0/17　　B．60.15.2.0/17
　　C．60.15.100.0/17　　D．60.15.128.0/17

**试题（52）分析**

第一个子网为 60.15.0.0/17　　**0011 1100.0000 1111．**0000 0000.0000 0000

则另一个子网为 60.15.128.0/17　　**0011 1100.0000 1111．**1000 0000.0000 0000

**参考答案**

（52）D

**试题（53）、（54）**

假设用户 X 有 4000 台主机，则必须给他分配__（53）__个 C 类网络。如果为其分配的网络号为 196.25.64.0，则给该用户指定的地址掩码为__（54）__。

（53）A．4　　B．8　　C．10　　D．16

（54）A．255.255.255.0　　B．255.255.250.0
　　C．255.255.248.0　　D．255.255.240.0

**试题（53）、（54）分析**

用户 X 有 4000 台主机，则必须给他分配 16 个 C 类网络，253×16=4048。给该用户指定的地址掩码为 255.255.240.0，其二进制表示形式为：

1111 1111.1111 1111.**1111 0000**.0000 0000

第三个字节的前四位为子网掩码的一部分，第三个字节的后四位用于区分 16 个不同的 C 类网络。

**参考答案**

（53）D　（54）D

**试题（55）、（56）**

如果在查找路由表时发现有多个选项匹配，那么应该根据__（55）__原则进行选择。假设路由表有 4 个表项如下所示，那么与地址 139.17.179.92 匹配的表项是__（56）__。

（55）A．包含匹配　　B．恰当匹配　　C．最长匹配　　D．最短匹配

（56）A．139.17.145.32　　B．139.17.145.64
　　C．139.17.147.64　　D．139.17.177.64

**试题（55）、（56）分析**

查找路由表时如发现有多个选项匹配，那么应该根据最长匹配原则进行选择。列出的 4 个表项中，与地址 139.17.179.92 匹配的表项是 139.17.177.64，参见下面的二进制

表示。

路由表项 139.17.145.32 的二进制表示为：**1000 1011.0001 0001.10**01 0001.0010 0000

路由表项 139.17.145.64 的二进制表示为：**1000 1011.0001 0001.10**01 0001.0100 0000

路由表项 139.17.147.64 的二进制表示为：**1000 1011.0001 0001.10**01 0011.0100 0000

路由表项 139.17.177.64 的二进制表示为：**1000 1011.0001 0001.1011 00**01.0100 0000

地址 139.17.179.92 的二进制表示为：　**1000 1011.0001 0001.1011 00**11.0100 0000

显然与最后一个表项为最长匹配。

**参考答案**

（55）C　（56）D

**试题（57）**

配置路由器接口的提示符是__（57）__。

（57）A．router（config）#　　B．router（config-in）#

C．router（config-intf）#　　D．router（config-if）#

**试题（57）分析**

路由器的配置操作有 3 种模式，即用户执行模式、特权模式和配置模式。在用户执行模式下，用户只能发出有限的命令，这些命令对路由器的正常工作没有影响；在特权模式下，用户可以发出丰富的命令，以便更好地控制和使用路由器；在配置模式下，用户可以创建和更改路由器的配置，对路由器的管理和配置主要在配置模式下完成。配置模式又分为全局配置模式和接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

- Router> 路由器处于用户执行模式状态，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。
- Router# 路由器处于特权模式状态，在 Router>提示符下输入 enable，可进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。
- Router(config)# 路由器处于全局配置模式状态，在 Router#提示符下输入 configure terminal，可进入全局设置状态，这时可以设置路由器的全局参数。
- Router(config-if)#，router(config-line)#，router(config-router)#，… 路由器处于局部设置状态，这时可以设置路由器某个局部的参数。
- > 路由器处于 RXBOOT 状态，在开机后 60s 内按 Ctrl+Break 组合键可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。或者进行路由器口令恢复时要进入该状态。
- 设置对话状态 这是一台新路由器开机时自动进入的状态，在特权命令状态使用 setup 命令也可进入此状态。用户可以通过“yes”或者“no”选择是否使用设置对话方式对路由器进行管理和配置。

**参考答案**

（57）D

**试题（58）**

如果想知道配置了哪种路由协议，应使用的命令是 （58） 。

（58）A．router>show router protocol

B．Router（config）>show ip protocol

C．router（config）>#show router protocol

D．router>show ip protocol

**试题（58）分析**

显示路由协议的命令是 router>show ip protocol。

**参考答案**

（58）D

**试题（59）**

如果在互联网中添加了一个局域网，要用手工方式将该局域网添加到路由表中，应使用的命令是 （59） 。

（59）A．router（config）>ip route 2.0.0.0 255.0.0.0 via 1.0.0.2

B．router（config）#ip route 2.0.0.0 255.0.0.0 1.0.0.2

C．router（config）#ip route 2.0.0.0 via 1.0.0.2

D．router（config）#ip route 2.0.0.0 1.0.0.2 mask 255.0.0.0

**试题（59）分析**

用手工方式将局域网添加到路由表中使用的命令是：

router（config）#ip route 2.0.0.0 255.0.0.0 1.0.0.2

**参考答案**

（59）B

**试题（60）、（61）**

IPv6 地址的格式前缀（FP）用于表示 （60） 。为了实现 IP 地址的自动配置，IPv6 主机将 （61） 附加在地址前缀 1111 1110 10 之后，产生一个链路本地地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。

（60）A．地区号　　B．地址类型或子网地址

C．网络类型　　D．播送方式或子网号

（61）A．32 位二进制随机数　　B．主机名字

C．网卡 MAC 地址　　D．IPv4 地址

**试题（60）、（61）分析**

IPv6 地址的格式前缀（FP）用于表示地址类型或子网地址。为了实现 IP 地址的自动配置，IPv6 主机将 MAC 地址附加在地址前缀 1111 1110 10 之后，产生一个链路本地

地址，如果通过了邻居发现协议的验证，则表明自我配置的链路本地地址是有效的。

**参考答案**

（60）B　（61）C

**试题（62）**

以下关于 CSMA/CD 协议的叙述中，正确的是（62）。

（62）A. 每个结点按照逻辑顺序占用一个时间片轮流发送
B. 每个结点检查介质是否空闲，如果空闲则立即发送
C. 每个结点想发就发，如果没有冲突则继续发送
D. 得到令牌的结点发送，没有得到令牌的结点等待

**试题（62）分析**

以太网 CSMA/CD 协议的工作原理如下。工作站在发送数据之前，先监听信道上是否有别的站发送的载波信号。若有，说明信道忙；否则信道是空闲的。即使信道空闲，若立即发送仍然会发生冲突。所以需要监听算法把冲突概率减到最小。有以下 3 种监听算法：

1. 非坚持型监听算法：当一个站准备好帧，在发送之前先监听信道。

① 若信道空闲，立即发送，否则转②。

② 若信道忙，则后退一个随机时间，重复①。

由于随机时延后退，从而减少了冲突的概率。然而，可能会因为后退而使信道闲置一段时间，这使信道的利用率降低，而且增加了发送时延。

2. 1-坚持型监听算法：当一个站准备好帧，发送之前先监听信道。

① 若信道空闲，立即发送，否则转②。

② 若信道忙，继续监听，直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间。但是，多个站同时都在监听信道时必然发生冲突。

3. P-坚持型监听算法。这种算法汲取了以上两种算法的优点，但较为复杂：

① 若信道空闲，以概率 P 发送，以概率（1－P）延迟一个时间单位。一个时间单位等于网络传输时延 $\tau$。

② 若信道忙，继续监听直到信道空闲，转①。

③ 如果发送延迟一个时间单位 $\tau$，则重复①。

载波监听只能减小冲突的概率，不能完全避免冲突。当两个帧发生冲突后，若继续发送，将会浪费网络带宽。为了进一步改进带宽的利用率，发送站应采取边发边听的冲突检测方法，即：

① 发送期间同时接收，并把接收的数据与站中存储的数据进行比较。（或用其他办法检测冲突）

② 若比较结果一致，说明没有冲突，重复①。

③ 若比较结果不一致，说明发生了冲突，立即停止发送，并发送一个简短的阻塞信号（Jamming），使所有站都停止发送。

④ 发送 Jamming 信号后，等待一段随机长的时间，重新监听，再试图发送。

**参考答案**

（62）B

**试题（63）**

以下关于交换机获取与其端口连接设备的 MAC 地址的叙述中，正确的是<u>（63）</u>。

（63）A. 交换机从路由表中提取设备的 MAC 地址

B. 交换机检查端口流入分组的源地址

C. 交换机之间互相交换地址表

D. 由网络管理员手工输入设备的 MAC 地址

**试题（63）分析**

交换机获取与其端口连接的设备的 MAC 地址的方法是检查端口流入分组的源地址，并将其记录在地址表中。

**参考答案**

（63）B

**试题（64）、（65）**

ITU-R 对 4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是<u>（64）</u>，选定的多路复用技术是<u>（65）</u>。

（64）A. 10Mb/s　　B. 100Mb/s　　C. 20Mb/s　　D. 1Gb/s

（65）A. OFDM　　B. QPSK　　C. MIMO　　D. 64-QAM

**试题（64）、（65）分析**

4G 标准的要求是能够提供基于 IP 的高速语音、数据和流式多媒体服务，支持的数据速率至少是 100Mb/s，选定的多路复用技术是 OFDM（正交频分多路复用）。

**参考答案**

（64）B　（65）A

**试题（66）**

用来承载多个 VLAN 流量的协议组是<u>（66）</u>。

（66）A. 802.11a 和 802.1q　　B. ISL 和 802.1q

C. ISL 和 802.3ab　　D. SSL 和 802.11b

**试题（66）分析**

802.1q 是标准的 IEEE 协议，用于区分不同的 VLAN。802.1q 在以太网帧的源MAC 地址和 Type 字段之间插入 4 个字节的 Tag 字段（最大帧长为 1522 字节）。Tag 字段里包括priority（0～7）和 VLAN ID（0～4095），其中 VLAN ID=0 用于识别优先级，VLAN ID=4095 保留未用，所以最多可配置 4094 个 VLAN。

ISL（Inter-Switch Link）是 Cisco 专有的Trunk封装方式，是在以太网帧的最前面加上 26 字节的帧头，在以太网帧的后面加上 4 字节的CRC 校验（最大帧长为 1548 字节）。在新加的帧头里有 15 比特用来标识 VLAN，但目前只用到低 10 位，所以最多可以区分 1024 个 VLAN。

**参考答案**

（66）B

**试题（67）**

多协议标记交换（MPLS）是 IETF 提出的第三层交换标准，以下关于 MPLS 的叙述中，正确的是＿（67）＿。

（67）A．带有 MPLS 标记的分组封装在 PPP 帧中传输

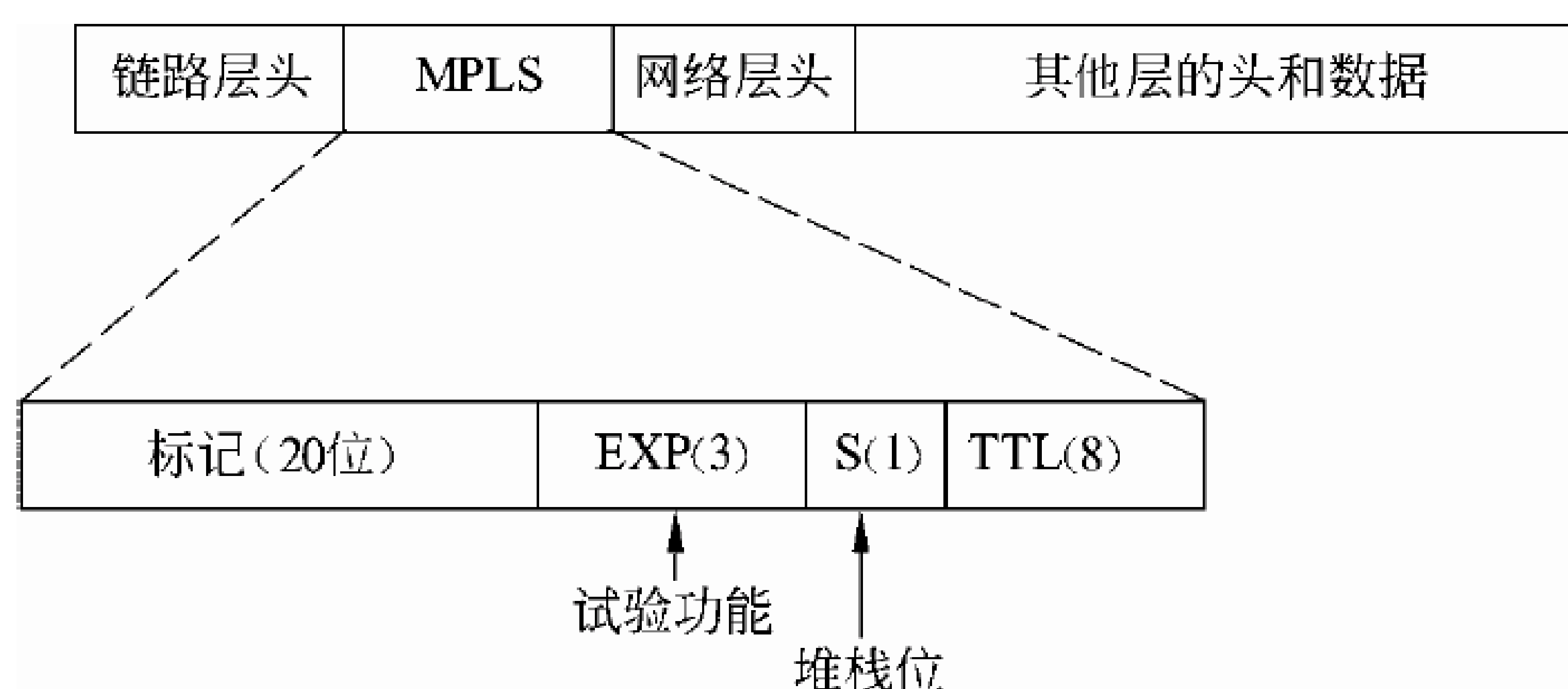
B．传送带有 MPLS 标记的分组之前先要建立对应的网络连接

C．路由器根据转发目标把多个 IP 流聚合在一起组成转发等价类

D．MPLS 标记在各个子网中是特定分组的唯一标识

**试题（67）分析**

IETF 开发的多协议标记交换（MPLS）把第 2 层的链路状态信息（带宽、延迟、利用率等）集成到第 3 层的协议数据单元中，从而简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层，标准格式如下图所示。

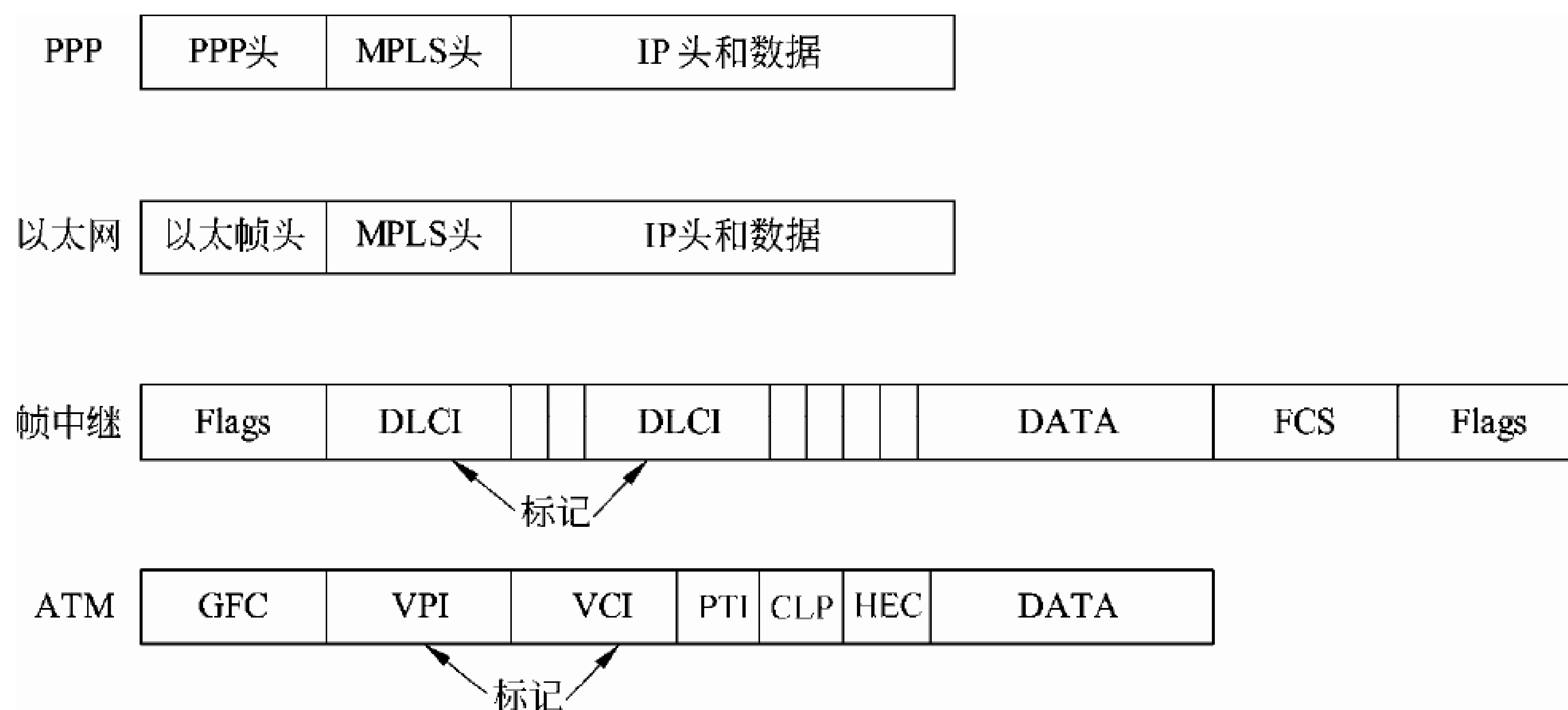



MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等，如下图所示。

当分组进入 MPLS 网络时，标记边缘路由器（LER）就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽和延迟等），而且还引用了 IP 头中的源地址字段、传输层端口号和服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路（LSP）中，标记交换路由器（LSR）将根据标记来处置分组，不再经过第 3 层转发，从而加快了网络的传输速度。

MPLS 可以把多个通信流汇聚成为一个转发等价类（FEC）。LER 根据目标地址和端

口号把分组指派到一个等价类中，在 LSR 中只需根据等价类标记查找标记信息库（LIB），确定下一跳的转发地址。这样使得协议更具伸缩性。MPLS 标记具有局部性，一个标记只是在一定的传输域中有效。




**参考答案**

（67）C

**试题（68）、（69）**

通过 HFC 网络实现宽带接入，用户端需要的设备是__（68）__，局端用于控制和管理用户的设备是__（69）__。

（68）A．Cable Modem　　B．ADSL Modem
　　C．OLT　　D．CMTS

（69）A．Cable Modem　　B．ADSL Modem
　　C．OLT　　D．CMTS

**试题（68）、（69）分析**

通过 HFC 网络实现宽带接入，用户端需要的设备是 Cable Modem，局端用于控制和管理用户的设备是 CMTS，如下图所示。

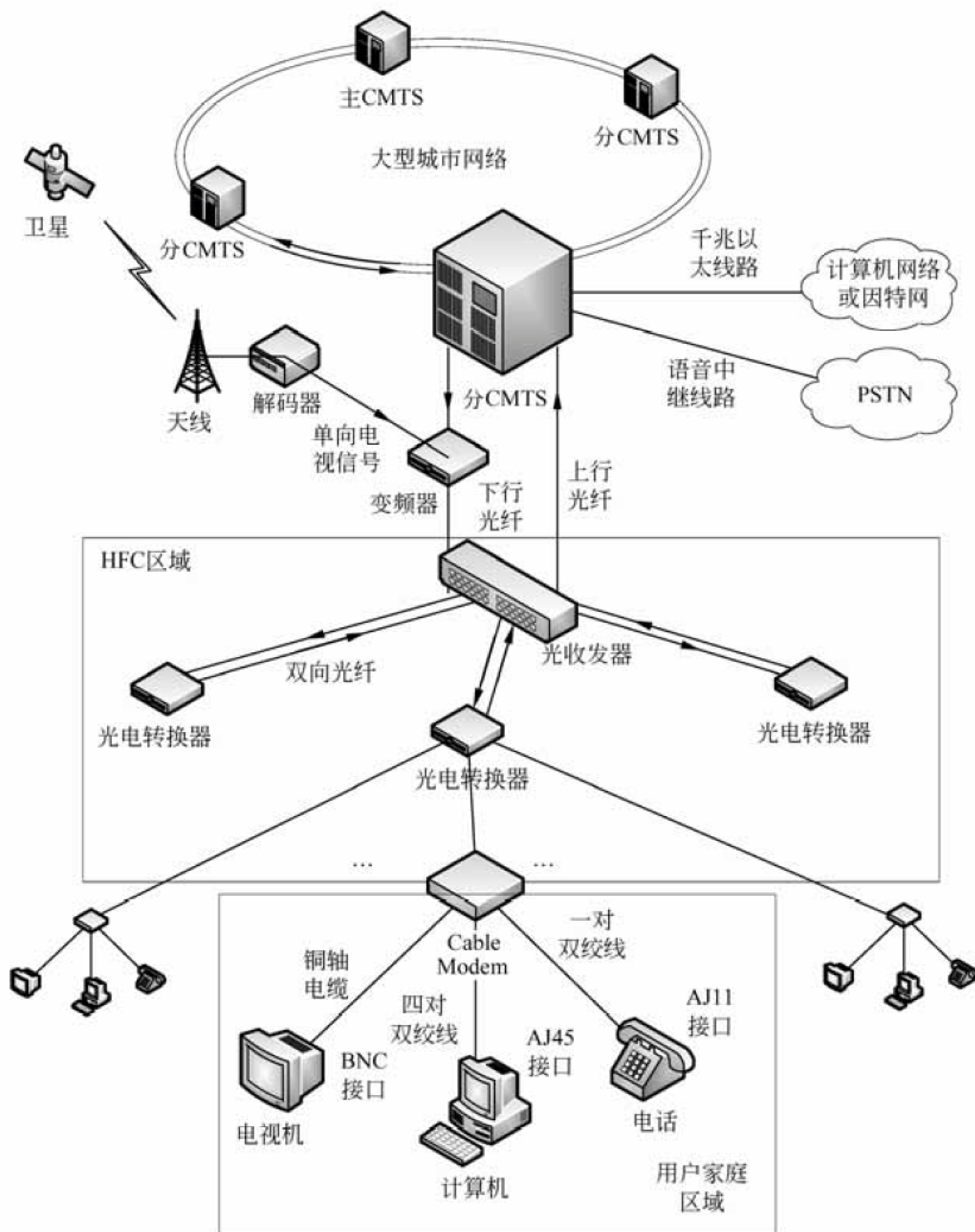
**参考答案**

（68）A　（69）D

**试题（70）**

在层次化局域网模型中，以下关于核心层的叙述中，正确的是__（70）__。

（70）A．为了保障安全性，对分组要进行有效性检查
　　B．将分组从一个区域高速地转发到另一个区域
　　C．由多台二、三层交换机组成
　　D．提供多条路径来缓解通信瓶颈




**试题（70）分析**

在层次化局域网模型中，核心层的主要功能是将分组从一个区域高速地转发到另一个区域。核心层是因特网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

汇聚层是核心层和接入层的分界点，应尽量将资源访问控制、核心层流量的控制等都在汇聚层实施。汇聚层应向核心层隐藏接入层的详细信息，汇聚层向核心层路由器进行路由宣告时，仅宣告多个子网地址汇聚而形成的一个网络。另外，汇聚层也会对接入层屏蔽网络其他部分的信息，汇聚层路由器可以不向接入路由器宣告其他网络部分的路

由，而仅仅向接入设备宣告自己为默认路由。

接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户之间的互访需要，并且为这些访问提供足够的带宽。接入层还应该适当负责一些用户管理功能，包括地址认证、用户认证和计费管理等内容。接入层还负责一些信息的用户信息收集工作，例如用户的 IP 地址、MAC 地址和访问日志等信息。

**参考答案**

（70）B

**试题（71）～（75）**

The Dynamic Host Configuration Protocol provides configuration parameters to Internet （71）. DHCP consists of two components: a （72） for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver （73） parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a （74） IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time. In "manual allocation", a client's IP address is assigned by the network （75）, and DHCP is used simply to convey the assigned address to the client.

（71）A. switch　B. terminal　C. hosts　D. users

（72）A. router　B. protocol　C. host　D. mechanism

（73）A. control　B. broadcast　C. configuration　D. transmission

（74）A. permanent　B. dynamic　C. connection　D. session

（75）A. controller　B. user　C. host　D. administrator

**参考译文**

动态主机配置协议向因特网主机提供配置参数。DHCP 由两个部分组成：一个用于从 DHCP 服务器向主机提交主机专用配置参数的协议，以及一种给主机分配网络地址的机制。DHCP 建立在客户机-服务器模式上，专用的 DHCP 服务器负责分配网络地址，并且向动态配置的主机提交配置参数。DHCP 支持 3 种 IP 地址分配机制。在“自动分配”方式中，DHCP 为客户指定一个固定的 IP 地址。在“动态分配”模式中，DHCP 给客户分配一个仅在一定时间段内有效的 IP 地址。在“手工分配”模式中，客户的 IP 地址是由网络管理员指定的，DHCP 只是把分配的地址转送给客户。

**参考答案**

（71）C　（72）B　（73）C　（74）A　（75）D

# 第 28 章　2015 下半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某工业园区视频监控网络拓扑如图 1-1 所示。

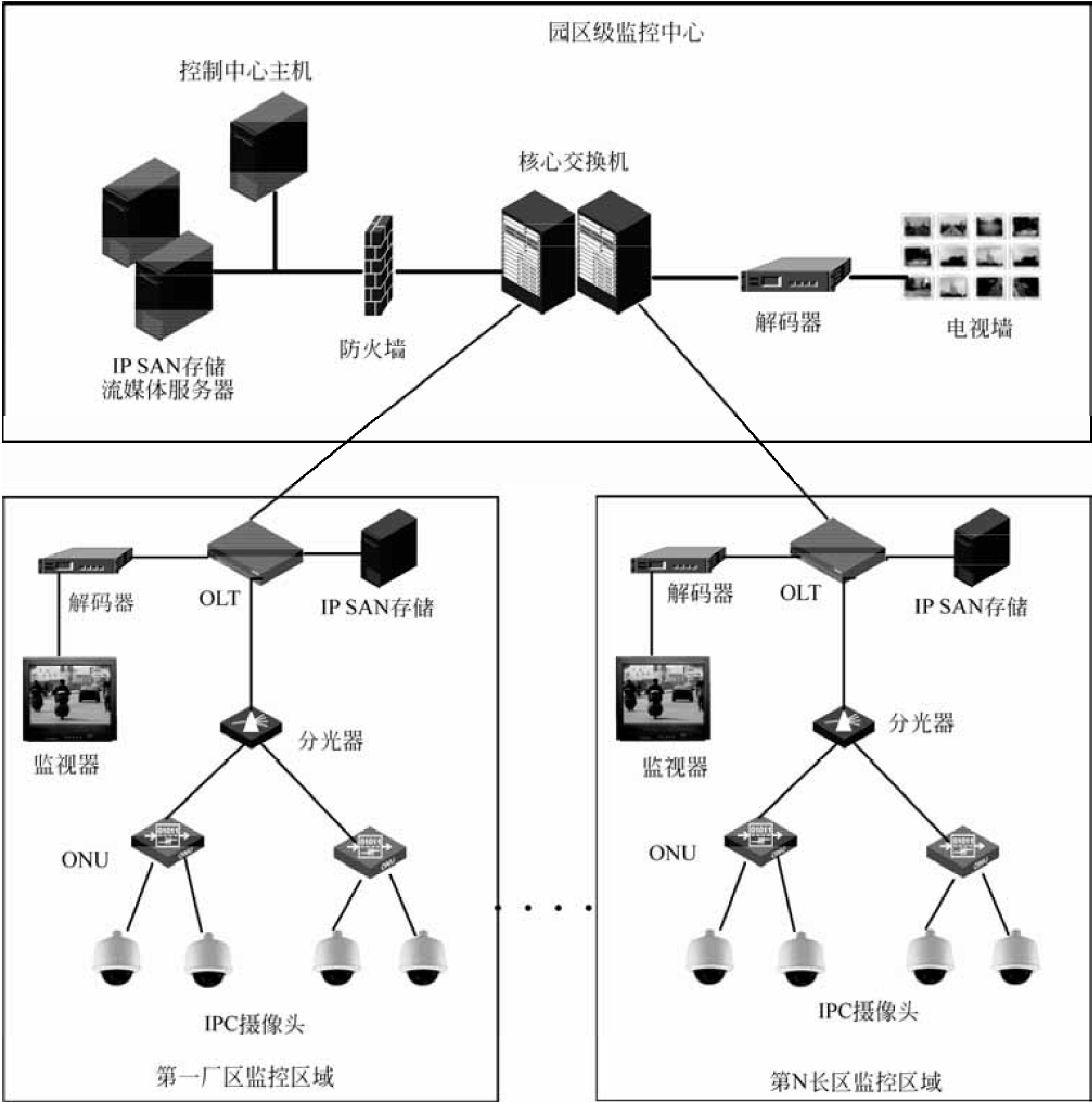



图 1-1

**【问题 1】（4 分）**

图 1-1 中使用了 SAN 存储系统，SAN 是一种连接存储管理子系统和__（1）__的专用网络。SAN 分为 FC SAN 和 IP SAN，其中 FC SAN 采用__（2）__互联；IP SAN 采用__（3）__互联；SAN 可以被看作是数据传输的后端网络，而前端网络则负责正常的__（4）__传输。

（1）～（4）备选答案：

A. iSCSI　　B. TCP/IP　　C. 以太网技术
D. SATA　　E. 文件服务器　　F. 光纤通道技术
G. 视频管理子系统　　H. 存储设备

**【问题 2】（4 分）**

该网络拓扑是基于 EPON 的技术组网，与传统的基于光纤收发器的组网有所不同。请从组网结构复杂度、设备占用空间大小、设备投资多少、网络管理维护难易程度等几方面对两种网络进行比较。

**【问题 3】（6 分）**

1．该系统采用 VLAN 来隔离各工厂和监控点，在__（5）__端进行 VLAN 配置，在__（6）__端采用 trunk 进行 VLAN 汇聚，使用 Manage VLAN 统一管理 OLT 设备。

2．OLT 的 IP 地址主要用于设备的网元管理，一般采用__（7）__方式分配，IPC 摄像机的地址需要统一规划，各厂区划分为不同的地址段。

**【问题 4】（6 分）**

1．在视频监控网络中，当多个监控中心同时查看一个点的视频时要求网络支持__（8）__。

（8）备选答案：

A. IP 广播　　B. IP 组播　　C. IP 任意播

2．在组网时，ONU 设备的__（9）__接口通过 UTP 网线和 IPC 摄像机连接。

（9）备选答案：

A. BNC　　B. RJ45　　C. USB

3．该网络的网管解决方案中一般不包含__（10）__功能或组件。

（10）备选答案：

A. 网元管理　　B. 防病毒模块
C. EPON 系统管理　　D. 事件、告警管理

**试题一分析**

本题通过视频监控网络的组网环境，考查 EPON 的特点与组网的相关知识。

此类题目要求考生熟悉网络系统的优化、网络存储和组网的基本技术，并且在工程实践中灵活运用。

**【问题 1】**

SAN（Storage Area Network）存储区域网络，是一种高速的、专门用于存储操作的网络，通常独立于计算机局域网（LAN）。SAN 将主机和存储设备连接在一起，能够为其上的任意一台主机和任意一台存储设备提供专用的通信通道。SAN 将存储设备从服务

器中独立出来，实现了服务器层次上的存储资源共享。SAN 将通道技术和网络技术引入存储环境中，提供了一种新型的网络存储解决方案，能够同时满足吞吐率、可用性、可靠性、可扩展性和可管理性等方面的要求。

SAN 分为 FC SAN 和 IP SAN，其中 FC SAN 采用光纤通道技术互联；IP SAN 采用以太网技术互联；SAN 可以被看作是数据传输的后端网络，而前端网络则负责正常的 TCP/IP 传输。

**【问题 2】**

EPON（Ethernet Passive Optical Network，以太网无源光网络）源于以太网的 PON 技术。它采用点到多点结构、无源光纤传输，在以太网之上提供多种业务。综合了 PON 技术和以太网技术的优点：低成本、高带宽、扩展性强、与现有以太网兼容、方便管理等。

光纤收发器，是一种将短距离的双绞线电信号和长距离的光信号进行互换的以太网传输媒体转换单元。一般应用在以太网电缆无法覆盖、必须使用光纤来延长传输距离的实际网络环境中，且通常定位于宽带城域网的接入层应用，成对使用。

**【问题 3】**

在 ONU 设备上配置 VLAN 用户和业务，在 OLT 设备上将相同的 VLAN 配置在同一个逻辑通道中。IP 地址的分配分为动态或静态，OLT 的地址用于设备的管理，应采用静态方式。

**【问题 4】**

TCP/IP 传输方式有 3 种：单播、广播、组播。单播在发送和每个接收主机之间需要单独的数据信道，如果有多个主机希望获得数据包的同一份拷贝将导致发送端负担沉重、延迟长、网络拥塞。组播是允许一个或多个主机发送一个数据包到多个主机的网络技术。组播源把数据包发送到特定组播组，只有属于该组播组地址的主机才能接收到数据包。广播是指在 IP 子网内广播数据包，所有在子网内部的主机都将收到这些数据包。

UTP 网线由一定长度的双绞线和 RJ-45 水晶头组成。双绞线由 8 根不同颜色的线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。

防病毒模块属于网络安全防护的范畴，随着网络病毒特征的变化需要不断地升级病毒库。该模块与具体的网络设备的配置管理、运行维护和故障监控之间密切度不高，一般不作为特定网络管理解决方案的组成部分。

**参考答案**

**【问题 1】**

（1）H　（2）F　（3）C　（4）B

**【问题 2】**

| 对比内容 | 光纤收发器 | EPON |
|---|---|---|
| 组网结构 | 复杂 | 简单 |
| 占用空间 | 较多 | 较少 |
| 设备投资 | 较多 | 较少 |
| 管理维护 | 复杂 | 简单 |

【问题 3】

1．（5）ONU　（6）OLT

2．（7）静态或指定

【问题 4】

1．（8）B

2．（9）B

3．（10）B

**试题二（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某企业的网络结构如图 2-1 所示。

该企业通过一台路由器接入到互联网，企业内部按照功能的不同分为 6 个 VLAN。分别是网络设备与网管（VLAN1）、内部服务器（VLAN2）、Internet 连接（VLAN3）、财务部（VLAN4）、市场部（VLAN5）、研发部门（VLAN6）。

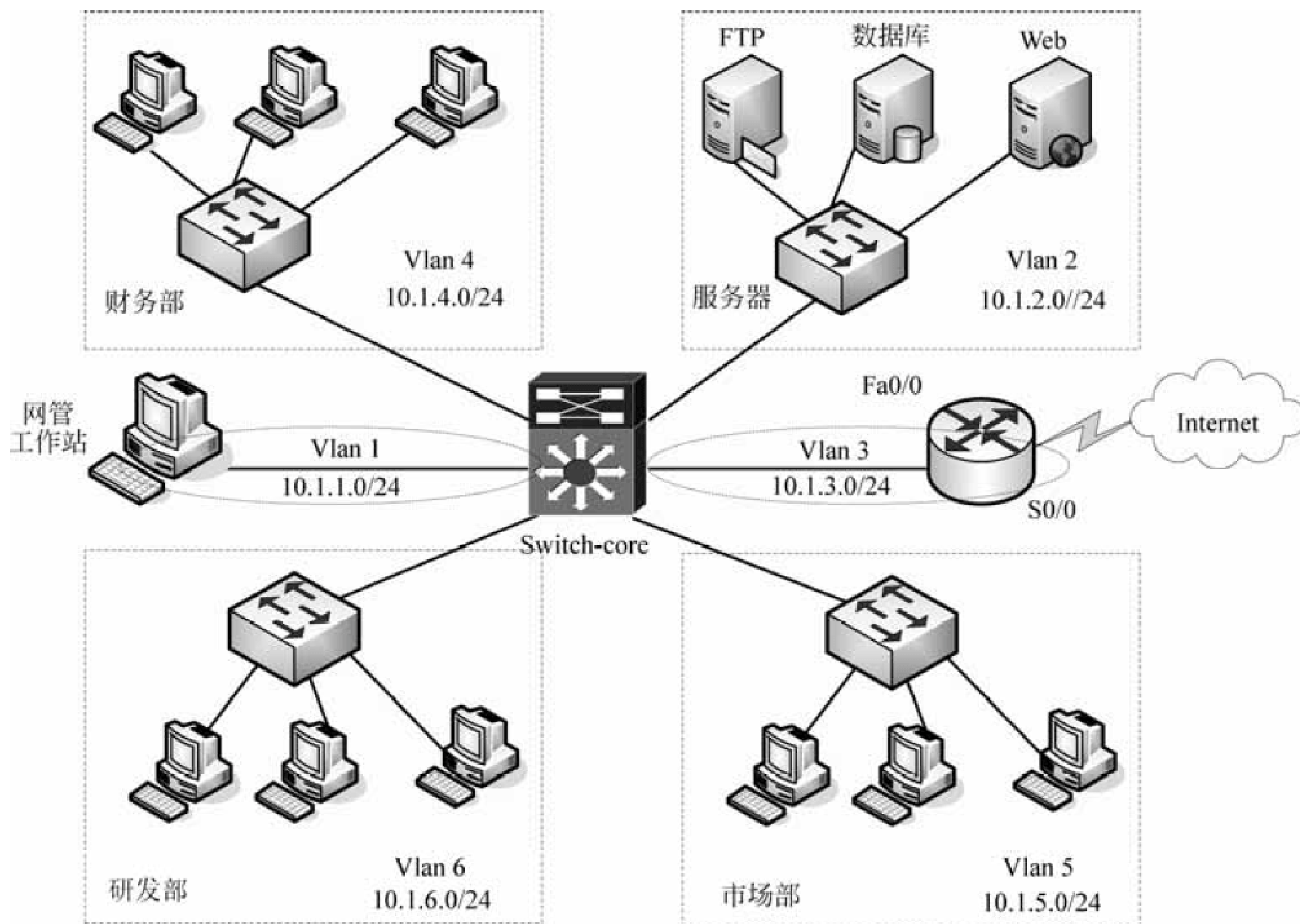



图 2-1　某企业网络拓扑图

【问题 1】（7 分）

1．访问控制列表 ACL 是控制网络访问的基本手段，它可以限制网络流量，提高网

络性能。ACL 使用__（1）__技术来达到访问控制目的。ACL 分为标准 ACL 和扩展 ACL 两种，标准访问控制列表的编号为__（2）__和 1300~1999 之间的数字，标准访问控制列表只使用__（3）__进行过滤，扩展的 ACL 的编号使用__（4）__以及 2000~2699 之间的数字。

2．每一个正确的访问列表都至少应该有一条__（5）__语句，具有严格限制条件的语句应放在访问列表所有语句的最上面，在靠近__（6）__的网络接口上设置扩展 ACL，在靠近__（7）__的网络接口上设置标准 ACL。

**【问题 2】（5 分）**

网管要求除了主机 10.1.6.66 能够进行远程 telnet 到核心设备外，其他用户都不允许进行 telnet 操作。同时只对员工开放 Web 服务器（10.1.2.20）、FTP 服务器（10.1.2.22）和数据库服务器（10.1.2.21:1521），研发部除 IP 为 10.1.6.33 的计算机外，都不能访问数据库服务器，按照要求补充完成以下配置命令。

```
…
Switch-core#conf t
Switch-core(config)#access-list 1 permit host  (8)
Switch-core(config)#line  (9)  0 4
Switch-core(config-line)#access-class 1  (10)
…
Switch-core(config)#ip access-list extend server-protect
Switch-core(config-ext-nacl)#permit tcp host  (11)  host 10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#deny tcp  (12)  0.0.0.255 host 10.1.2.21 eq
1521
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.21 eq 1521
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.20 eq www
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.22 eq ftp
…
```

**【问题 3】（4 分）**

该企业要求在上班时间内（9:00-18:00）禁止内部员工浏览网页（TCP 80 和 TCP 443 端口），禁止使用 QQ（TCP/UDP 8000 端口以及 UDP 4000）和 MSN（TCP 1863 端口）。另外在 2015 年 6 月 1 日到 2 日的所有时间内都不允许进行上述操作。除上述限制外，在任何时间都允许以其他方式访问 Internet。为了防止利用代理服务访问外网，要求对常用的代理服务端口 TCP 8080、TCP 3128 和 TCP 1080 也进行限制。按照要求补充完成（或解释）以下配置命令。

```
…
Switch-core(config)#time-range TR1
Switch-core(config-time-range)#absolute start 00:00 1 June 2015 end 00:00
3 June 2015
Switch-core(config-time-range)#periodic weekdays start __(13)__
Switch-core(config-time-range)#exit
…
Switch-core(config)#ip access-list extend internet_limit
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 80
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 443
time-range TR1
//__(14)__
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1863
time-range TR1
//__(15)__
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 4000
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 3128
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8080
time-range TR1
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1080
time-range TR1
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int__(16)__
Switch-core(config-if)#ip access-group internet_limit out
…
```

**【问题 4】（4 分）**

企业要求市场和研发部门不能访问财务部 VLAN 中的数据，但是财务部门作为公司的核心管理部门，又必须能访问到市场和研发部门 VLAN 内的数据。按照要求补充完成（或解释）以下配置命令。

```
…
Switch-core(config)#ip access-list extend fi-main
```

```
Switch-core(config-ext-nacl)#permit tcp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 120
Switch-core(config-ext-nacl)#permit udp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 200
Switch-core(config-ext-nacl)#permit icmp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 10
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int (17)
Switch-core(config-if)#ip access-group fi-main in
…
Switch-core(config)#ip access-list extend fi-access-limit
Switch-core(config-ext-nacl)#evaluate r-main
Switch-core(config-ext-nacl)#deny ip any (18)
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int (19)
Switch-core(config-if)#ip access-group fi-access-limit in
Switch-core(config-if)#int (20)
Switch-core(config-if)#ip access-group fi-access-limit in
```

**试题二分析**

本题考查网络层访问权限控制技术 ACL 的使用配置。

此类题目要求考生不但具有较高的网络配置理论水平，而且必须具备较强的动手配置能力。

**【问题 1】**

本问题主要考查考生对 ACL 基本概念的掌握和应用。

信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。访问控制列表（Access Control List，ACL）是路由器和交换机接口的指令列表，用来控制端口进出的数据包。配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。如可以配置 ACL，禁止局域网内的设备访问外部公共网络，或者只能使用 FTP 服务。

ACL 使用包过滤技术，在路由器上读取第 3 层及第 4 层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分为标准 ACL 和扩展 ACL 两种，标准访问控制列表的编号为 1～99 和 1300～1999 之间的数字，标准访问控制列表只使用源地址进行过滤，扩展的 ACL 的编号使用 100～199 以及 2000～2699 之间的数字。

在实施 ACL 的过程中，应当遵循如下两个基本原则：最小特权原则，只给受控对象完成任务所必须的最小的权限；最靠近受控对象原则，所有的网络层访问权限控制每一个正确的访问列表都至少应该有一条允许语句，具有严格限制条件的语句应放在访问列表所有语句的最上面，在靠近源地址的网络接口上设置扩展 ACL，在靠近目的地址的网络接口上设置标准 ACL。

**【问题 2】**

本问题主要考查考生对 ACL 基本配置命令的掌握和应用。

```
…
Switch-core#conf t
//进入全局配置模式
Switch-core(config)#access-list 1 permit host 10.1.6.66
//配置标准 acl1 允许源地址为 10.1.6.66 的包通过
Switch-core(config)#line vty 0 4
//进入 VTY 端口，对 VTY 端口进行配置
Switch-core(config-line)#access-class 1 in
//只允许 acl1 进入
…
Switch-core(config)#ip access-list extend server-protect
//定义扩展 ACL server-protect
Switch-core(config-ext-nacl)#permit tcp host 10.1.6.33 host 10.1.2.21 eq
1521
//允许主机 10.1.6.33 访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#deny tcp 10.1.6.0  0.0.0.255 host 10.1.2.21
eq 1521
//不允许 10.1.6.0 子网主机访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.21 eq 1521
//允许 10.1.0.0 子网的主机访问 10.1.2.21 的 1521 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.20 eq www
//允许 10.1.0.0 子网的主机访问 10.1.2.20 的 www 端口
Switch-core(config-ext-nacl)#permit  tcp  10.1.0.0  0.0.255.255  host
10.1.2.22 eq ftp
//允许 10.1.0.0 子网的主机访问 10.1.2.22 的 ftp 端口
…
```

**【问题 3】**

本问题主要考查考生使用 ACL 技术对网络访问进行精细化控制的能力。

```
…
Switch-core(config)#time-range TR1
```

```
//定义一个新的时间范围 TR1
Switch-core(config-time-range)#absolute start 00:00 1 June 2015 end 00:00
3 June 2015
//绝对时间范围为 2015 年 6 月 1 日到 2 日
Switch-core(config-time-range)#periodic weekdays start 9:00 18:00
//定义周期性重复使用的时间范围周一至周五 9:00-18:00
Switch-core(config-time-range)#exit
…
Switch-core(config)#ip access-list extend internet_limit
//定义扩展 ACL internet_limit
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 80
time-range TR1
//禁止以 http 浏览网页
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 443
time-range TR1
//禁止以安全方式浏览网页
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1863
time-range TR1
//禁止使用 MSN
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 8000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny udp 10.1.0.0 0.0.255.255 any eq 4000
time-range TR1
//禁止使用 QQ
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 3128
time-range TR1
//禁止使用代理端口 3128
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 8080
time-range TR1
//禁止使用代理端口 8080
Switch-core(config-ext-nacl)#deny tcp 10.1.0.0 0.0.255.255 any eq 1080
time-range TR1
//禁止使用代理端口 1080
Switch-core(config-ext-nacl)#permit ip any any
//允许所有数据通过
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int s0/0
//进入端口 s0/0 配置子模式
```

```
Switch-core(config-if)#ip access-group internet_limit out
//将 ACL internet_limit 应用在 s0/0 出口上
…
```

【问题 4】

本问题主要考查考生使用 IP ACL 实现单向访问控制的命令。

```
…
Switch-core(config)#ip access-list extend fi-main
//定义扩展 ACL fi-main
Switch-core(config-ext-nacl)#permit tcp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 120
//允许 tcp 流量，建立自反访问控制列表 r-main，没有流量的情况下 120 秒消失
Switch-core(config-ext-nacl)#permit udp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 200
//允许 udp 流量，建立自反访问控制列表 r-main，没有流量的情况下 200 秒消失
Switch-core(config-ext-nacl)#permit icmp any 10.1.0.0 0.0.255.255 reflect
r-main timeout 10
//允许 icmp 流量，建立自反访问控制列表 r-main，没有流量的情况下 10 秒消失
Switch-core(config-ext-nacl)#permit ip any any
//允许所有流量通过
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int vlan 4
//进入 VLAN4 子接口配置模式
Switch-core(config-if)#ip access-group fi-main in
//把 acl fi-main 应用在入口
…
Switch-core(config)#ip access-list extend fi-access-limit
//定义扩展 ACL fi-access-limit
Switch-core(config-ext-nacl)#evaluate r-main
//有符合 r-main 这个 reflect 组中所定义的 acl 条目的流量发生时，在 evaluate 语句所
在的当前位置动态生成一条反向的 permit 语句
Switch-core(config-ext-nacl)#deny ip any 10.1.4.0 0.0.0.255
//禁止访问 10.1.4.0 网段
Switch-core(config-ext-nacl)#permit ip any any
Switch-core(config-ext-nacl)#exit
Switch-core(config)#int vlan 5
//进入 VLAN5 子接口配置模式
Switch-core(config-if)#ip access-group fi-access-limit in
//把 acl fi-access-limit 应用在入口
Switch-core(config-if)#int vlan 6
//进入 VLAN6 子接口配置模式
```

```
Switch-core(config-if)#ip access-group fi-access-limit in
//把 acl fi-access-limit 应用在入口
```

## 参考答案

**【问题 1】**

1. （1）包过滤　（2）1～99　（3）源地址　（4）100～199
2. （5）允许　（6）源地址　（7）目的地址

**【问题 2】**

（8）10.1.6.66　（9）vty　（10）in　（11）10.1.6.33　（12）10.1.6.0

**【问题 3】**

（13）9:00 18:00　（14）禁止以安全方式浏览网页

（15）禁止使用 MSN　（16）s0/0

**【问题 4】**

（17）vlan 4　（18）10.1.4.0 0.0.0.255

（19）vlan 5　（20）vlan 6

注：（19）、（20）答案可互换

## 试题三（共 20 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业采用 Windows Server 2003 配置了 Web、FTP 和邮件服务。

**【问题 1】（4 分）**

Web 的配置如图 3-1 和图 3-2 所示。

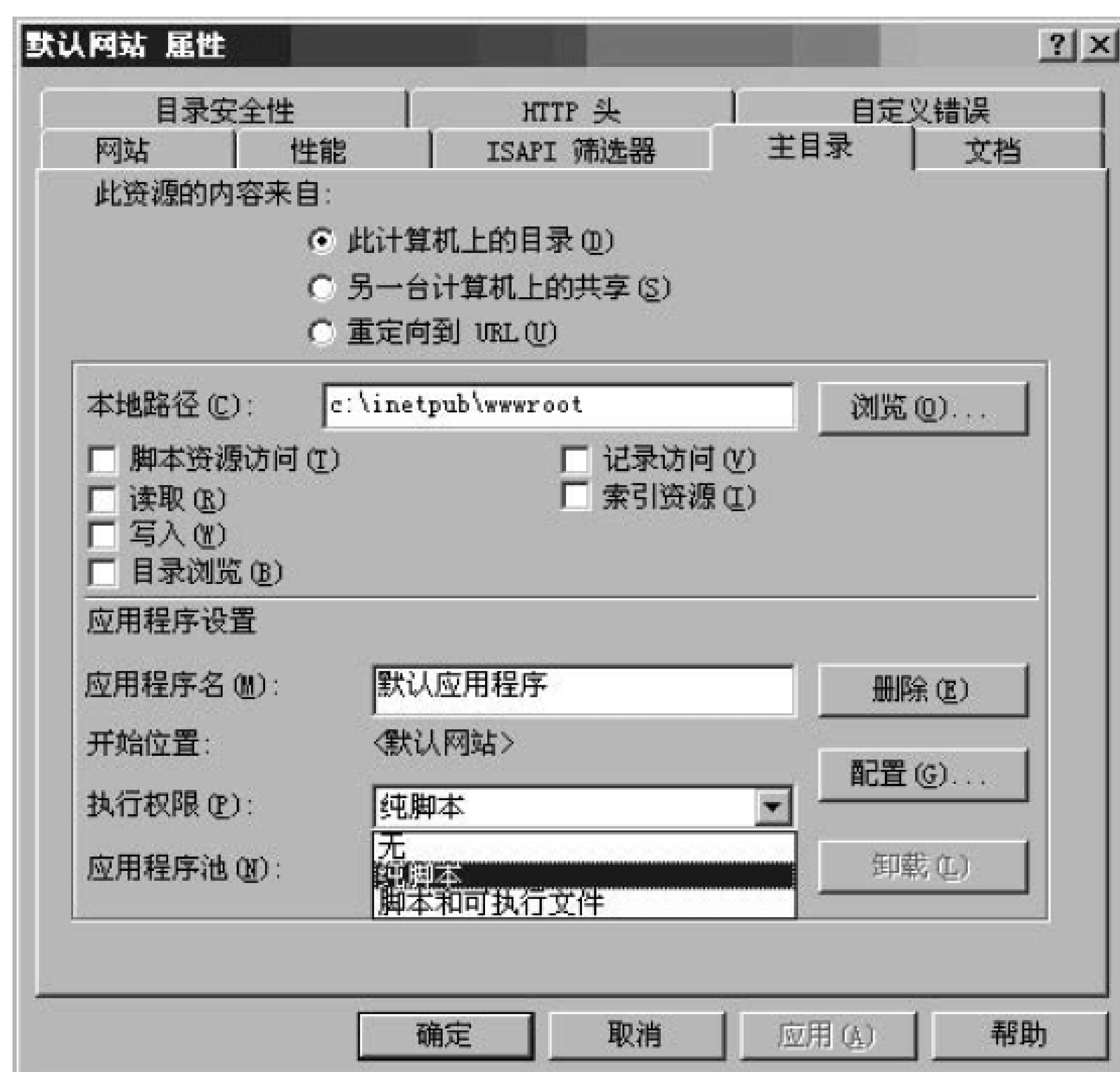



图 3-1

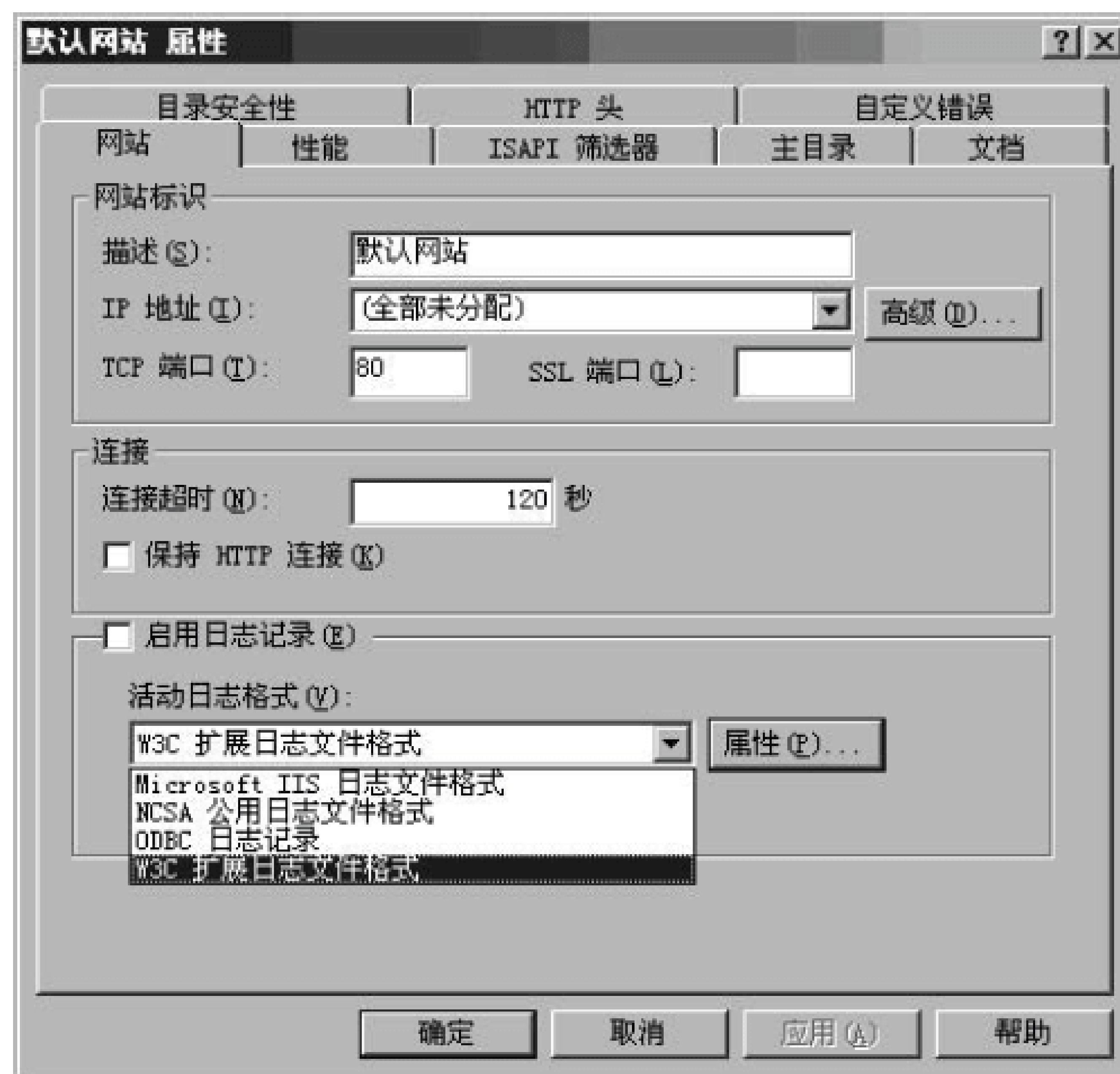



图 3-2

1．如果要记录用户访问历史，需__（1）__。

（1）备选答案：

A．同时勾选图 3-1 中“写入”复选框和图 3-2 中“启用日志记录”复选框

B．同时勾选图 3-1 中“记录访问”复选框和图 3-2 中“启用日志记录”复选框

C．同时勾选图 3-1 中“记录访问”复选框和“索引资源”复选框

D．同时勾选图 3-1 中“记录访问”复选框和图 3-2 中“保持 HTTP 连接”复选框

2．在图 3-2 所示的 4 种活动日志格式中，需要提供用户名和密码的是__（2）__。

**【问题 2】（4 分）**

根据图 3-1 判断正误。（正确的答“对”，错误的答“错”）

A．勾选“读取”是指禁止客户下载网页文件及其他文件。__（3）__

B．不勾选“写入”是指禁止客户以 HTTP 方式向服务器写入信息。__（4）__

C．勾选“目录浏览”是指当客户请求的文件不存在时，将显示服务器上的文件列表。__（5）__

D．当网页文件是 CGI 文件时，“执行权限”中选择“纯脚本”。__（6）__

**【问题 3】（6 分）**

FTP 的配置如图 3-3 所示。

匿名用户的权限与在“本地用户和组”的权限__（7）__，FTP 可以设置__（8）__虚拟目录。FTP 服务器可以通过__（9）__访问。

（9）备选答案：

A．DOS、客户端方式

B．客户端、浏览器方式

C．DOS、浏览器、客户端方式




图 3-3

**【问题 4】（6 分）**

邮件服务器的配置如图 3-4 所示。

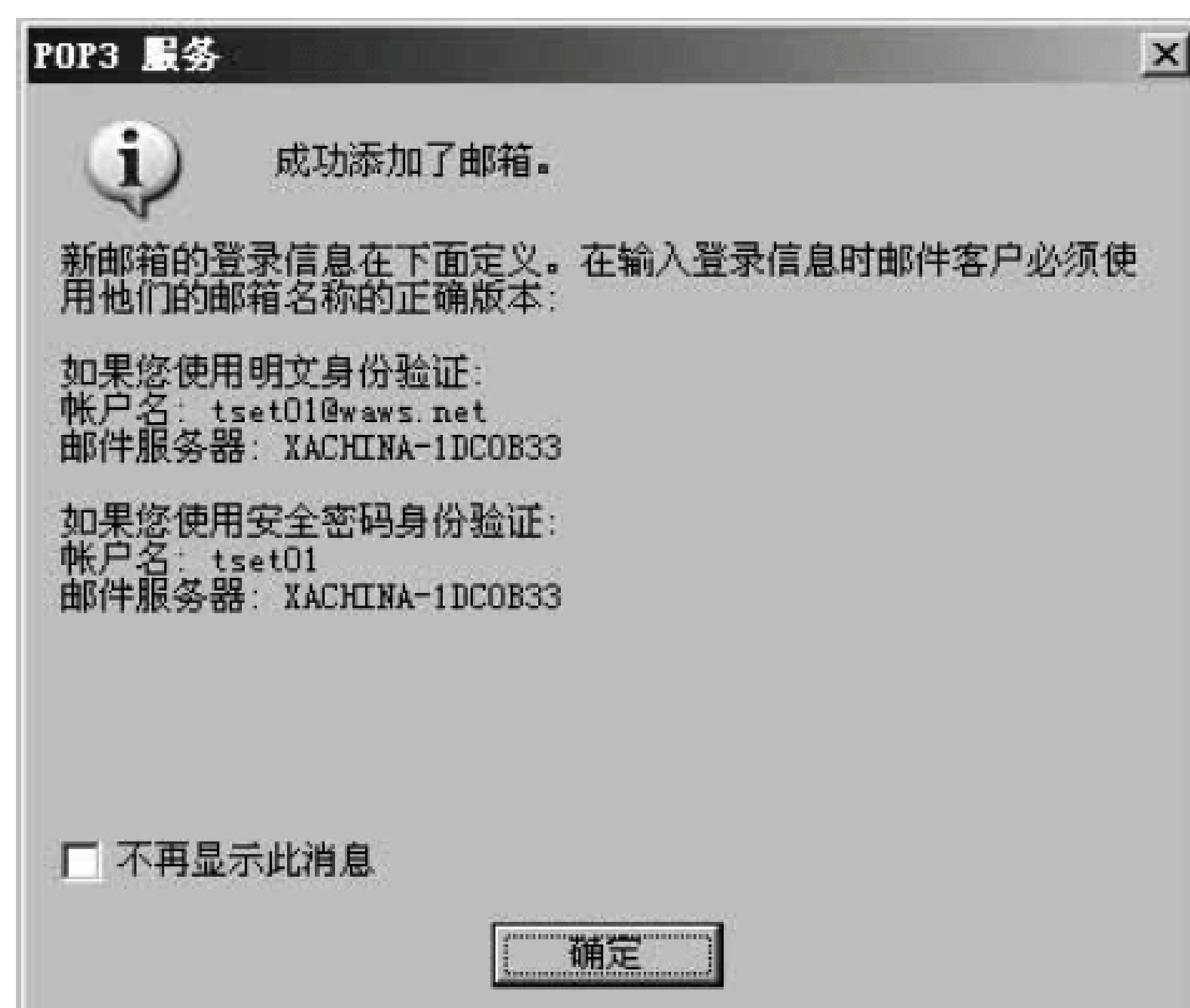



图 3-4

若图 3-4 所示 waws.net 域已经在 Internet 上注册，那么在 DNS 服务器中应配置邮件服务器的 （10） 记录。POP3 是 （11） 邮件协议，配置 POP3 服务器的步骤包含 （12）（多选）。

（11）备选答案：

A．接收　　B．发送　　C．存储　　D．转发

（12）备选答案：

A．创建邮件域　　B．设置服务器最大连接数

C．安装 POP3 组件　　D．添加邮箱

## 试题三分析

IIS 是微软推出的架设 WEB、FTP、SMTP 服务器的一整套系统组件，集成在 NT 核心的服务器系统中。本题考查 Windows 环境下 Web 服务、FTP 服务及邮件服务的安装与配置。

此类题目要求考生熟悉 Windows 环境提供的网络服务。了解安装网络服务时相关参数设置的含义和配置目的。

**【问题 1】**

在对 Web 的配置时，“默认网站 属性”页面是配置网站的主要页面。本题“记录用户访问历史”的作用是获得（IIS）日志记录，该记录可提供比 Windows Server 2003 的事件日志记录或性能监视功能更详细的信息。IIS 日志包括以下信息：访问网站的用户、他们查看的内容以及最后一次查看信息的时间等内容。需要注意的是必须同时选中“网站”选项卡上的“启用日志记录”和“主目录”选项卡上的“记录访问”才能启用日志记录。

如果选择了“ODBC 日志记录”，请单击“属性”，并提供 ODBC 数据源名称（DSN）、表、用户名和密码，然后单击“确定”。

**【问题 2】**

IIS Web 服务器的权限设置有两个方面，一个是 NTFS 文件系统本身的权限设置，另一个是“默认网站 属性”页面的“主目录”选项卡的设置。在“主目录”选项卡中选中“读取”“写入”“目录浏览”等设置都代表“允许”的含义。

在“执行权限”的选项中，网页文件是 CGI 文件时，需要选择“纯脚本和可执行程序”。

**【问题 3】**

在进行 FTP 的设置时，匿名用户使用的用户名和密码都来自“本地用户和组”，并且与“本地用户和组”中的权限一致。FTP 可以设置多个虚拟目录为不同的用户提供服务。FTP 可以通过命令行、浏览器、客户端方式访问。

**【问题 4】**

MX（Mail Exchanger）记录是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当 Internet 上的某用户要发一封信给 user@mydomain.com 时，该用户的邮件系统通过 DNS 查找 mydomain.com 这个域名的 MX 记录，如果 MX 记录存在，用户计算机就将邮件发送到 MX 记录所指定的邮件服务器上。

POP 是一种电子邮件传输协议，3 代表该协议第 3 个版本，规定了怎样将个人计算机连接到 Internet 邮件服务器和下载电子邮件的电子协议。配置 POP 包括安装组件、创建域、添加邮件等内容。“设置服务器最大连接数”是配置 SMTP 服务时配置的参数。

## 参考答案

**【问题 1】**

1. （1）B
2. （2）ODBC 日志记录

**【问题 2】**

（3）错　（4）对　（5）对　（6）错

**【问题 3】**

（7）相同　（8）多个　（9）C

**【问题 4】**

（10）MX　（11）A　（12）ACD

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司网络拓扑结构图如图 4-1 所示。公司内部的用户使用私有地址段 192.168.1.0/24。

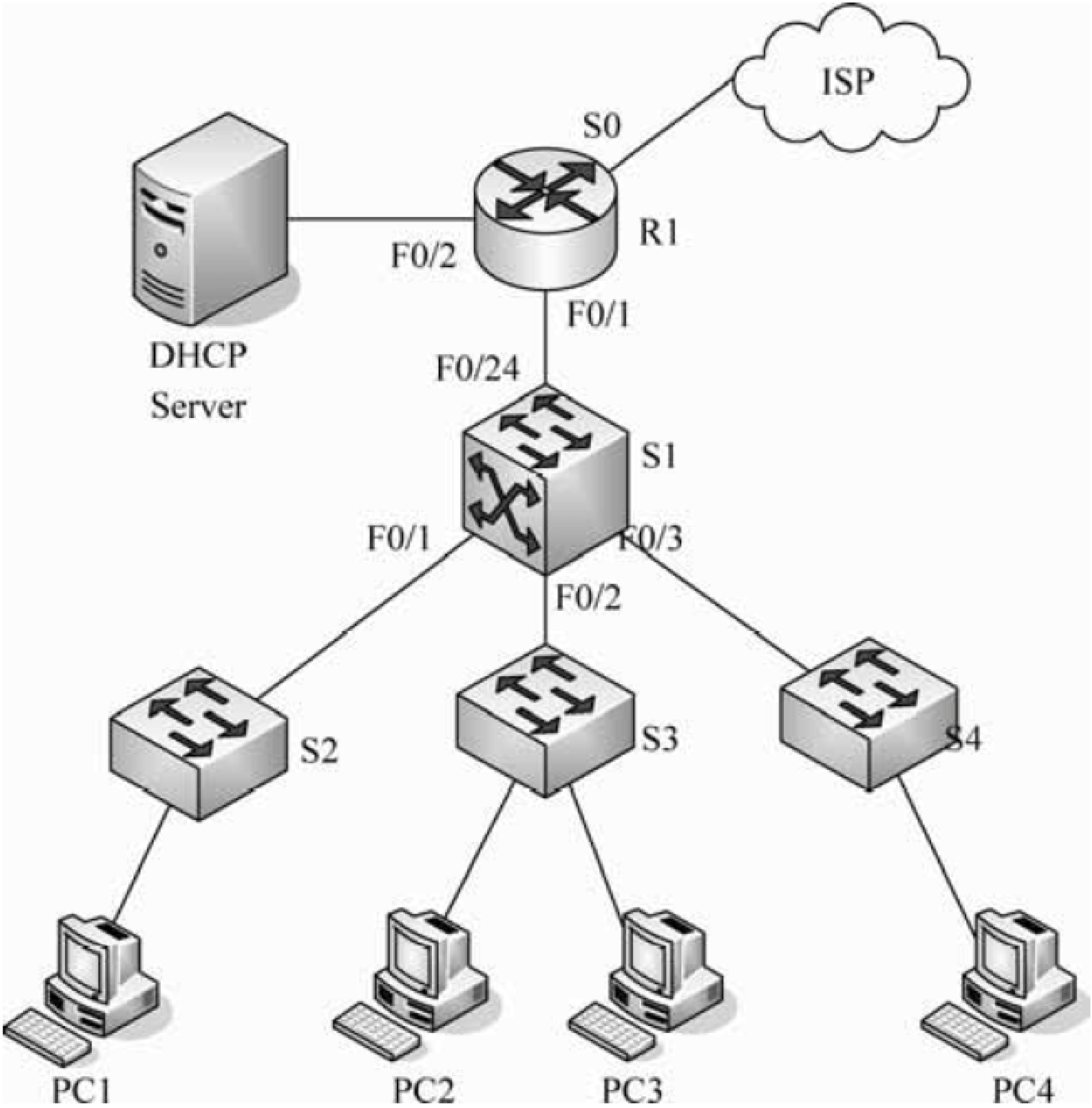



图 4-1

**【问题 1】（2 分）**

为节省 IP 地址，在接口地址上均使用 30 位地址掩码，请补充下表中的空白。

| 设备 | 接口 | IP 地址 | 设备 | 接口 | IP 地址 |
|---|---|---|---|---|---|
| S1 | F0/24 | 192.168.1.253 | R1 | F0/1 | （1） |
| DHCPServer | Eth0 | 192.168.1.249 | | F0/2 | （2） |

**【问题 2】（9 分）**

将公司内部用户按照部门分别划分在 3 个 vlan 中：vlan 10，vlan 20 和 vlan 30。均连接在交换机 S1 上，并通过 S1 实现 vlan 间通信，所有内网主机均采用 DHCP 获取 IP 地址。按照要求补充完成（或解释）以下配置命令。

```
Switch>en
Switch#__(3)__
Switch(config)#hostname __(4)__
S1(config)#interface fastEthernet 0/1
S1(config-if)#__(5)__ mode trunk
S1(config)#interface vlan 10      //__(6)__
S1(config-if)#ip address 192.168.1.206 255.255.255.240
S1(config-if)#no shutdown
S1(config-if)#ip helper-address __(7)__
S1(config-if)#__(8)__
S1(config)#
……
S1(config)#router __(9)__
S1(config-router)#version __(10)__
S1(config-router)#network 192.168.1.192
S1(config-router)#network 192.168.1.208
S1(config-router)#network 192.168.1.224
S1(config-router)#__(11)__
S1#
```

**【问题 3】（2 分）**

在 S1 上将 F0/1 接口配置为 trunk 模式时，出现了以下提示：

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

应采取__（12）__方法解决该问题。

（12）A. 在该接口上使用 no shutdown 命令后再使用该命令
B. 在该接口上启用二层功能后再使用该命令
C. 重新启动交换机后再使用该命令
D. 将该接口配置为 access 模式后再使用该命令

**【问题 4】（2 分）**

在 S1 上配置的 3 个 SVI 接口地址分别处在 192.168.1.192，192.168.1.208 和 192.168.1.224 网段，它们的子网掩码是__（13）__。

**试题四分析**

本题考查交换机的配置以及三层交换机中实现 VLAN 间路由的基本配置方法。

该类题目首先要求考生能够认真阅读题目，领会题目的要求，并熟悉相关设备的基

本配置命令和配置逻辑。

【问题 1】

问题 1 的说明中，已明确表示使用 30 位掩码作为设备之间连接时接口的 IP 地址。根据问题 1 中表格所示，已给出了对端的 IP 地址，并使用的是 30 位掩码，通过 IP 地址计算，可得路由器对应接口上的 IP 地址。

【问题 2】

根据问题 2 的描述可知，对交换机 S1 需要完成 VLAN 间路由、DHCP 中继和 RIP 协议的配置。其中，DHCP 中继需指明 DHCP 服务器的 IP 地址。在 RIP 协议的配置中，由于局域网地址均使用的是非主类地址，需要使用 RIPv2 版本才可以正确宣告路由。

【问题 3】

在三层交换机上，当交换机接口模式为“auto”模式时，无法直接将该接口模式配置为中继“trunk”模式，需先将该接口的模式手动调整为“access”模式后，再使用中继配置命令，将接口模式配置为中继模式。

【问题 4】

为了在交换机上实现 VLAN 间路由，需在交换机上设置 SVI（Switch Visual Interface）接口，3 个 SVI 接口处在 192.168.1.192，192.168.1.208 和 192.168.1.224 网段，将最后一个字节使用二进制表示后为：

192：11000000

208：11010000

224：11100000

可知，其子网掩码为 28 位掩码。

参考答案

【问题 1】

（1）192.168.1.254　（2）192.168.1.250

【问题 2】

（3）config terminal　（4）S1　（5）switchport

（6）创建 VLAN 10 接口　（7）192.168.1.249　（8）exit

（9）rip　（10）2　（11）end

【问题 3】

（12）D

【问题 4】

（13）255.255.255.240

# 第 29 章　2016 上半年网络工程师上午试题分析与解答

**试题（1）**

内存按字节编址，从 A1000H 到 B13FFH 的区域的存储容量为__（1）__kb。

（1）A．32　　B．34　　C．65　　D．67

**试题（1）分析**

本题考查计算及系统基础知识。

结束地址和起始地址的差值再加 1 为存储单元的个数，B13FFH−A1000H+1=10400H，转换为十进制后等于 65536+1024=64kb+1kb=65k。

**参考答案**

（1）C

**试题（2）**

以下关于总线的叙述中，不正确的是__（2）__。

（2）A．并行总线适合近距离高速数据传输

B．串行总线适合长距离数据传输

C．单总线结构在一个总线上适应不同种类的设备，设计简单且性能很高

D．专用总线在设计上可以与连接设备实现最佳匹配

**试题（2）分析**

本题考查计算机系统基础知识。

串行总线将数据一位一位传输，数据线只需要一根（如果支持双向需要 2 根），并行总线是将数据的多位同时传输（4 位，8 位，甚至 64 位，128 位），显然，并行总线的传输速度快，在长距离情况下成本高，串行传输的速度慢，但是远距离传输时串行成本低。

单总线结构在一个总线上适应不同种类的设备，通用性强，但是无法达到高的性能要求，而专用总线则可以与连接设备实现最佳匹配。

**参考答案**

（2）C

**试题（3）**

某软件公司参与开发管理系统软件的程序员张某，辞职到另一公司任职，于是该项目负责人将该管理系统软件上开发者的署名更改为李某（接张某工作）。该项目负责人的行为__（3）__。

（3）A．侵犯了张某开发者身份权（署名权）

B．不构成侵权，因为程序员张某不是软件著作权人

C．只是行使管理者的权利，不构成侵权

D．不构成侵权，因为程序员张某现已不是项目组成员

**试题（3）分析**

《计算机软件保护条例》规定软件著作权人享有的权利，包括发表权、署名权、修改权、复制权、发行权、出租权、信息网络传播权、翻译权。署名权是指软件开发者为表明身份在自己开发的软件原件及其复制件上标记姓名的权利。法律法规规定署名权的根本目的，在于保障不同软件来自不同开发者这一事实不被人混淆，署名即是标记，旨在区别，区别的目的是为了有效保护软件著作权人的合法权益。署名彰显了开发者与软件之间存在关系的客观事实。因此，行使署名权应当奉行诚实的原则，应当符合有效法律行为的要件，否则会导致署名无效的后果。

署名权只能是真正的开发者和被视同开发者的法人和非法人团体才有资格享有，其他任何个人、单位和组织不得行使此项权利。所以，署名权还隐含着另一种权利，即开发者资格权。法律保护署名权，意味着法律禁止任何未参加开发人在他人开发的软件上署名。《计算机软件保护条例》规定“在他人开发的软件上署名或者更改他人开发的软件上的署名”的行为是侵权行为，这种行为侵犯了开发者身份权即署名权。

**参考答案**

（3）A

**试题（4）**

以下媒体文件格式中__（4）__是视频文件格式。

（4）A．WAV　　B．BMP　　C．MP3　　D．MOV

**试题（4）分析**

WAV 是 Windows 操作系统采用的音频文件格式；BMP 是图像文件格式；MP3 是音频文件格式；MOV 是 Apple 公司开发的一种视频格式，默认的播放器是 QuickTimePlayer。具有较高的压缩比率和较完美的视频清晰度等特点，但是其最大的特点还是跨平台性，即不仅能支持 MacOS，同样也能支持 Windows 系列。

**参考答案**

（4）D

**试题（5）**

使用 150DPI 的扫描分辨率扫描一幅 3×4 英寸的彩色照片，得到原始的 24 位真彩色图像的数据量是__（5）__ Byte。

（5）A．1800　　B．90000　　C．270000　　D．810000

**试题（5）分析**

DPI（Dots Per Inch，每英寸点数）通常用来描述数字图像输入设备（如图像扫描仪）或点阵图像输出设备（点阵打印机）输入或输出点阵图像的分辨率。一幅 3×4 英寸的

彩色照片在 150DPI 的分辨率下扫描得到原始的 24 位真彩色图像的数据量是(150×3)×(150×4)×24/8= 810000 字节。

**参考答案**

（5）D

**试题（6）**

以下关于脚本语言的叙述中，正确的是__（6）__。

（6）A．脚本语言是通用的程序设计语言

B．脚本语言更适合应用在系统级程序开发中

C．脚本语言主要采用解释方式实现

D．脚本语言中不能定义函数和调用函数

**试题（6）分析**

本题考查程序语言基础知识。

维基百科上将脚本语言定义为“为了缩短传统的编写—编译—链接—运行过程而创建的计算机编程语言。通常具有简单、易学、易用的特色，目的就是希望开发者以简单的方式快速完成某些复杂程序的编写工作。”

脚本语言一般运行在解释器或虚拟机中，便于移植，开发效率较高。

**参考答案**

（6）C

**试题（7）、（8）**

在结构化分析中，用数据流图描述__（7）__。当采用数据流图对一个图书馆管理系统进行分析时，__（8）__是一个外部实体。

（7）A．数据对象之间的关系，用于对数据建模

B．数据在系统中如何被传送或变换，以及如何对数据流进行变换的功能或子功能，用于对功能建模

C．系统对外部事件如何响应，如何动作，用于对行为建模

D．数据流图中的各个组成部分

（8）A．读者　　B．图书　　C．借书证　　D．借阅

**试题（7）、（8）分析**

本题考查结构化分析的基础知识。

数据流图是结构化分析的一个重要模型，描述数据在系统中如何被传送或变换，以及描述如何对数据流进行变换的功能，用于功能建模。

数据流图中有四个要素：外部实体，也称为数据源或数据汇点，表示要处理的数据的输入来源或处理结果要送往何处，不属于目标系统的一部分，通常为组织、部门、人、相关的软件系统或者硬件设备；数据流表示数据沿箭头方向的流动；加工是对数据对象的处理或变换；数据存储在数据流中起到保存数据的作用，可以是数据库文件或者任何

形式的数据组织。

根据上述定义和题干说明，读者是外部实体，图书和借书证是数据流，借阅是加工。

**参考答案**

（7）B　（8）A

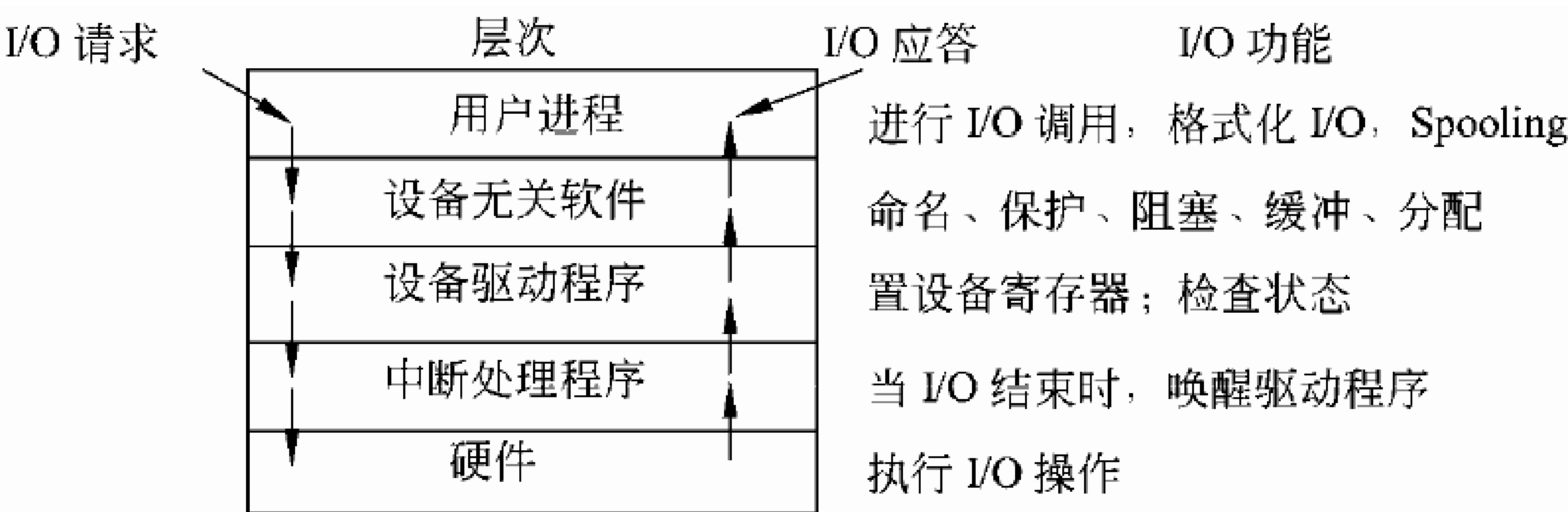
**试题（9）**

当用户通过键盘或鼠标进入某应用系统时，通常最先获得键盘或鼠标输入信息的是＿（9）＿程序。

（9）A．命令解释　　B．中断处理　　C．用户登录　　D．系统调用

**试题（9）分析**

I/O 设备管理软件一般分为 4 层：中断处理程序、设备驱动程序、与设备无关的系统软件和用户级软件。至于一些具体分层时细节上的处理，是依赖于系统的，没有严格的划分，只要有利于设备独立这一目标，可以为了提高效率而设计不同的层次结构。I/O 软件的所有层次及每一层的主要功能如下图所示。




图中的箭头给出了 I/O 部分的控制流。当用户通过键盘或鼠标进入某应用系统时，通常最先获得键盘或鼠标输入信息的程序是中断处理程序。

**参考答案**

（9）B

**试题（10）**

在 Windows 操作系统中，当用户双击“IMG_20160122_103.jpg”文件名时，系统会自动通过建立的＿（10）＿来决定使用什么程序打开该图像文件。

（10）A．文件　　B．文件关联　　C．文件目录　　D．临时文件

**试题（10）分析**

本题考查 Windows 操作系统文件管理方面的基础知识。

当用户双击一个文件名时，Windows 系统通过建立的文件关联来决定使用什么程序打开该文件。例如，系统建立了“Windows 照片查看器”或“11view”程序打开扩展名为“.jpg”类型的文件关联，那么当用户双击“IMG_20160122_103.jpg”文件时，Windows 先执行“Windows 照片查看器”或“11view”程序，然后打开“IMG_20160122_103.jpg”文件。

**参考答案**

（10）B

**试题（11）**

用于连接以太网的网桥类型是__（11）__。

（11）A. 源路由网桥　　B. 透明网桥
　　C. 翻译网桥　　D. 源路由透明网桥

**试题（11）分析**

透明网桥（或生成树网桥）以混杂方式工作，它接收 LAN 上传送的每一帧。当收到一帧时，网桥必须决定将其丢弃或是进行转发。如果要转发，则通过查表找到目标主机的输出端口。网桥的地址表是通过生成树算法自动建立的。透明网桥的优点是易于安装，只需插入电缆就可以自动工作，无须预先进行设置。但是这种网桥仅仅使用了网络拓扑结构的一个子集。在 802 委员会内部，支持 CSMA/CD 和令牌总线的人选择了透明网桥，而令牌环的支持者则倾向于源路由网桥。

源路由网桥的核心思想是假定每个主机都知道接收主机与自己是否处于同一 LAN 中。主机把发送到其他 LAN 的帧的目标地址高位设置成 1，另外还在帧头加进此帧应走的实际路径。源路由网桥见到目标地址高位为 1 的帧时，按预定的路径进行转发。实际上，在这种网络中，每个主机都按照源路由算法建立了以自己为根的生成树，而这些生成树利用了网络中的每一条连接。

**参考答案**

（11）B

**试题（12）**

以下关于以太网交换机地址学习机制的说法中，错误的是__（12）__。

（12）A. 交换机的初始 MAC 地址表为空
　　B. 交换机接收到数据帧后，如果没有相应的表项，则不转发该帧
　　C. 交换机通过读取输入帧中的源地址添加相应的 MAC 地址表项
　　D. 交换机的 MAC 地址表项是动态变化的

**试题（12）分析**

交换机就是一种由高速硬件构成的多端口网桥。交换机的初始 MAC 地址表为空，收到一个数据帧时将其源地址添加到自己的 MAC 地址表中，通过这种逆向学习算法逐步建立地址表。当收到的帧的目标地址不在 MAC 地址表中时，交换机将其广播发送到所有输出端口。

**参考答案**

（12）B

**试题（13）**

路由器包含多种端口以连接不同类型的网络设备，其中能够连接 DDN、帧中继、

X.25 和 PSTN 等广域网络的是__（13）__。

（13）A. 同步串口　　B. 异步串口　　C. AUX 端口　　D. Consol 端口

**试题（13）分析**

路由器不仅能实现局域网之间的连接，还能实现局域网与广域网、广域网与广域网之间的连接。路由器与广域网连接的端口称为 WAN 端口，路由器与局域网连接的端口称为 LAN 端口。常见的网络端口有以下几种。

① RJ-45 端口。这种端口通过双绞线连接以太网。10Base-T 的 RJ-45 端口标识为 ETH，而 100Base-TX 的 RJ-45 端口标识为 10/100bTX，这是因为快速以太网路由器采用 10/100Mb/s 自适应电路。

② AUI 端口。AUI 端口是一种 D 型 15 针连接器，用在令牌环网或总线型以太网中。路由器经 AUI 端口通过粗同轴电缆收发器连接 10Base-5 网络，也可以通过外接的 AUI-to-RJ-45 适配器连接 10Base-T 以太网，还可以借助其他类型的适配器实现与 10Base-2 细同轴电缆或 10Base-F 光缆的连接。

③ 高速同步串口。在路由器与广域网的连接中，应用最多的是高速同步串行口（Synchronous Serial Port），这种端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。通过这种端口所连接的网络两端要求同步通信，以很高的速率进行数据传输。

④ ISDN BRI 端口。这种端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 三个通道（2B+D）的总带宽为 144 kb/s，端口采用 RJ-45 标准，与 ISDN NT1 的连接使用 RJ-45-to-RJ-45 直通线。

⑤ 异步串口。异步串口（ASYNC）主要应用于连接 Modem，以实现远程计算机通过 PSTN 拨号接入。异步端口的速率不是很高，也不要求同步传输，只要求能连续通信就可以了。

⑥ Console 端口。Console 端口通过配置专用电缆连接至计算机串行口，利用终端仿真程序（如 Windows 中的超级终端）对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。

⑦ AUX 端口。对路由器进行远程配置时要使用 AUX 端口（Auxiliary Prot）。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行电路转换。AUX 端口支持硬件流控。

**参考答案**

（13）A

**试题（14）**

通过正交幅度调制技术把 ASK 和 PSK 两种调制模式结合起来组成 16 种不同的码元，这时数据速率是码元速率的__（14）__倍。

（14）A. 2　　B. 4　　C. 8　　D. 16

**试题（14）分析**

所谓正交幅度调制（Quadrature Amplitude Modulation，QAM），就是把两个幅度相同但相位相差 90° 的模拟信号合成为一个模拟信号。下表的例子是把 ASK 和 PSK 技术结合起来，形成幅度相位复合调制，这也是一种正交幅度调制技术。由于形成了 16 种不同的码元，所以每一个码元可以表示 4 位二进制数据，使得数据速率大大提高。

**表　幅度相位复合调制**

| 二进制数 | 码元幅度 | 码元相位 | 二进制数 | 码元幅度 | 码元相位 |
|---|---|---|---|---|---|
| 0000 | $\sqrt{2}$ | 45° | 1000 | $3\sqrt{2}$ | 45° |
| 0001 | 3 | 0° | 1001 | 5 | 0° |
| 0010 | 3 | 90° | 1010 | 5 | 90° |
| 0011 | $\sqrt{2}$ | 135° | 1011 | $3\sqrt{2}$ | 135° |
| 0100 | 3 | 270° | 1100 | 5 | 270° |
| 0101 | $\sqrt{2}$ | 315° | 1101 | $3\sqrt{2}$ | 315° |
| 1010 | $\sqrt{2}$ | 225° | 1110 | $3\sqrt{2}$ | 225° |
| 0111 | 3 | 180° | 1111 | 5 | 180° |

**参考答案**

（14）B

**试题（15）、（16）**

一对有效码字之间的海明距离是__（15）__。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，最少需要增加的校验位是__（16）__位。

（15）A．两个码字的比特数之和　　B．两个码字的比特数之差
　　C．两个码字之间相同的位数　　D．两个码字之间不同的位数

（16）A．3　　B．4　　C．5　　D．6

**试题（15）、（16）分析**

海明（Hamming）研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字。码字之间的海明距离是一个码字要变成另一个码字时必须改变的最小位数。例如，7 位 ASCII 码增加一位奇偶位成为 8 位的码字，这 128 个 8 位的码字之间的海明距离是 2。所以，当其中 1 位出错时便能检测出来。两位出错时就变成另外一个码字了。

如果对于 $m$ 位的数据，增加 $k$ 位冗余位，则组成 $n=m+k$ 位的纠错码。对于 $2^m$ 个有效码字中的每一个，都有 $n$ 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错。这样，对于一个有效的消息总共有 $n+1$ 个可识别的码字。这 $n+1$ 个码字相对于其他 $2^m-1$ 个有效消息的距离都大于 1。这意味着总共有 $2^m(n+1)$个有效的或是可纠错的码字。显然，这个数应小于等于码字的所有可能的个数，即 $2^n$。于是，有

$$2^m(n+1)\leqq 2^n$$

因为 $n=m+k$，得出

$$m+k+1\leqq 2^k$$

对于给定的数据位 $m$，上式给出了 $k$ 的下界，即要纠正单个错误，$k$ 必须取的最小值。在本题中 $m$=10，可知 $k$=4。

**参考答案**

（15）D　（16）B

**试题（17）**

T1 载波的数据速率是＿（17）＿。

（17）A．1.544Mb/s　B．6.312Mb/s　C．2.048Mb/s　D．44.736Mb/s

**试题（17）分析**

T1 载波也叫一次群，它把 24 路话音信道按时分多路的原理复合在一条高速信道上。该系统的工作是这样的，用一个编码解码器轮流对 24 路话音信道取样、量化和编码，一个取样周期中（125μs）得到的 7 位一组的数字组合成一串，共 7×24 位长。这样的数字串在送入高速信道前要在每一个 7 位组的后面插入一个信令位，于是变成了 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 125μs 传送一帧，其中包含了各路话音信道的一组数字，还包含总共 24 位的控制信息以及 1 位帧同步信息。这样，不难算出 T1 载波的各项比特率。对每一路话音信道来说，传输数据的比特率为 7b/125μs=56 kb/s，传输控制信息的比特率为 1 b/125μs=8 kb/s，总的比特率为 193 b/125μs=1.544 Mb/s。

**参考答案**

（17）A

**试题（18）**

在 xDSL 技术中，能提供上下行信道非对称传输的技术是＿（18）＿。

（18）A．HDSL　B．ADSL
　　C．SDSL　D．ISDN DSL

**试题（18）分析**

数字用户线路（Digital Subscriber Line，DSL）允许用户在传统的电话线上提供高速的数据传输，用户计算机借助于 DSL 调制解调器连接到电话线上，通过 DSL 连接访问因特网络或者企业网络。

DSL 采用尖端的数字调制技术，可以提供比 ISDN 快得多的速率，其实际速率取决于 DSL 的业务类型和很多物理层因素，例如电话线的长度、线径、串扰和噪音等。

DSL 技术存在多种类型，以下是常见的技术类型。

- ADSL：非对称 DSL，上下行流量不对称，一般具有三个信道，分别为 1.544～9Mb/s 的高速下行信道，16～640kb/s 的双工信道，64kb/s 的语音信道。

- SDSL：对称 DSL，用户的上下行流量对称，最高可以达到 1.544Mb/s。
- ISDN DSL：介于 ISDN 和 DSL 之间，可以提供最远距离为 4600～5500m 的 128kb/s 双向对称传输。
- HDSL：高比特率 DSL，是在两个线对上提供 1.544Mb/s 或在三个线对上提供 2.048Mb/s 对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为 3700～4600m。
- VDSL：甚高比特率 DSL，一种快速非对称 DSL 业务，可以在一对电话线上提供数据和语音业务。

**参考答案**

（18）B

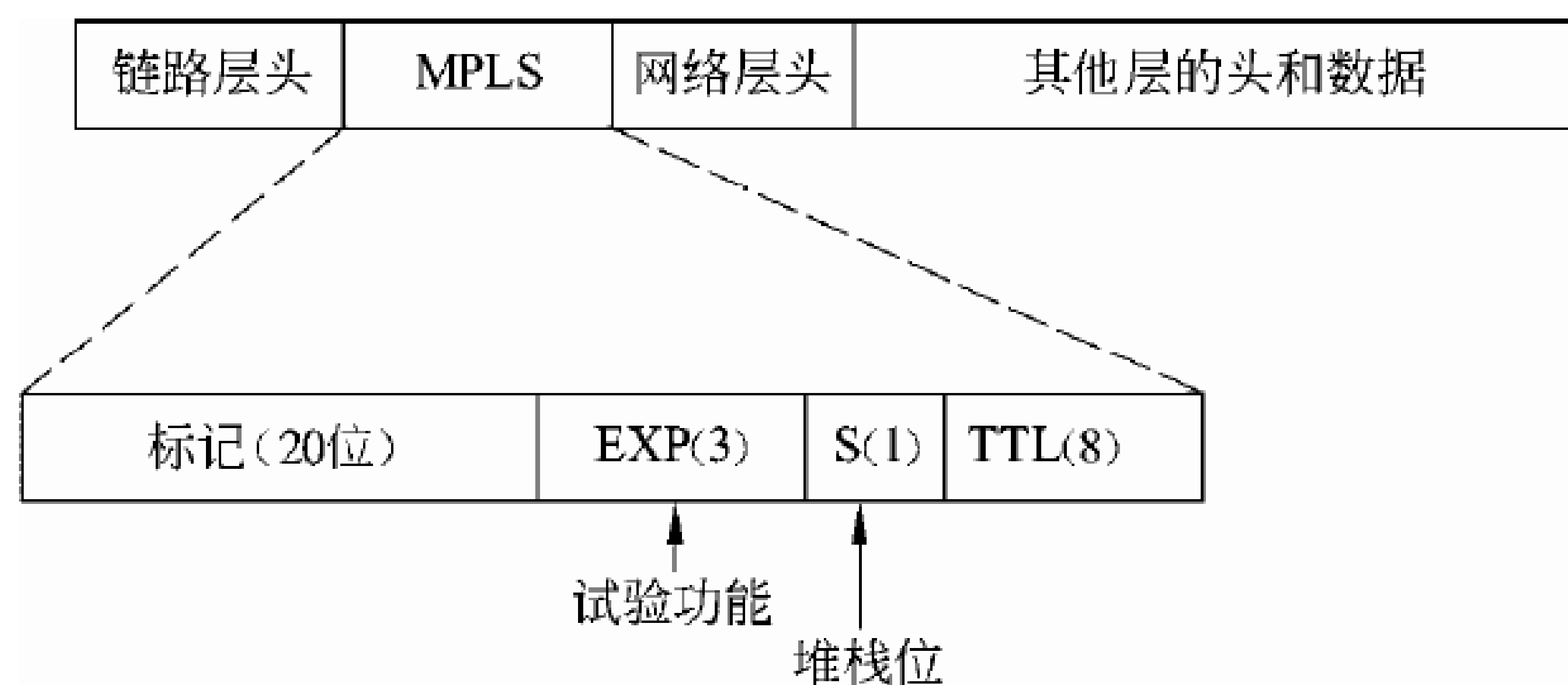
**试题（19）**

IETF 开发的多协议标记交换（MPLS）改进了第 3 层分组的交换过程。MPLS 包头的位置在__（19）__。

（19）A．第二层帧头之前　　B．第二层和第三层之间
　　C．第三层和第四层之间　　D．第三层头部中

**试题（19）分析**

IETF 开发的多协议标记交换（Multiprotocol Label Switching，MPLS，RFC3031）把第 2 层的链路状态信息（带宽、延迟、利用率等）集成到第 3 层的协议数据单元中，从而简化和改进了第 3 层分组的交换过程。理论上，MPLS 支持任何第 2 层和第 3 层协议。MPLS 包头的位置界于第 2 层和第 3 层之间，可称为第 2.5 层，标准格式如下图所示。MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包、甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等。




**参考答案**

（19）B

**试题（20）**

建立组播树是实现组播传输的关键技术，利用组播路由协议生成的组播树是__（20）__。

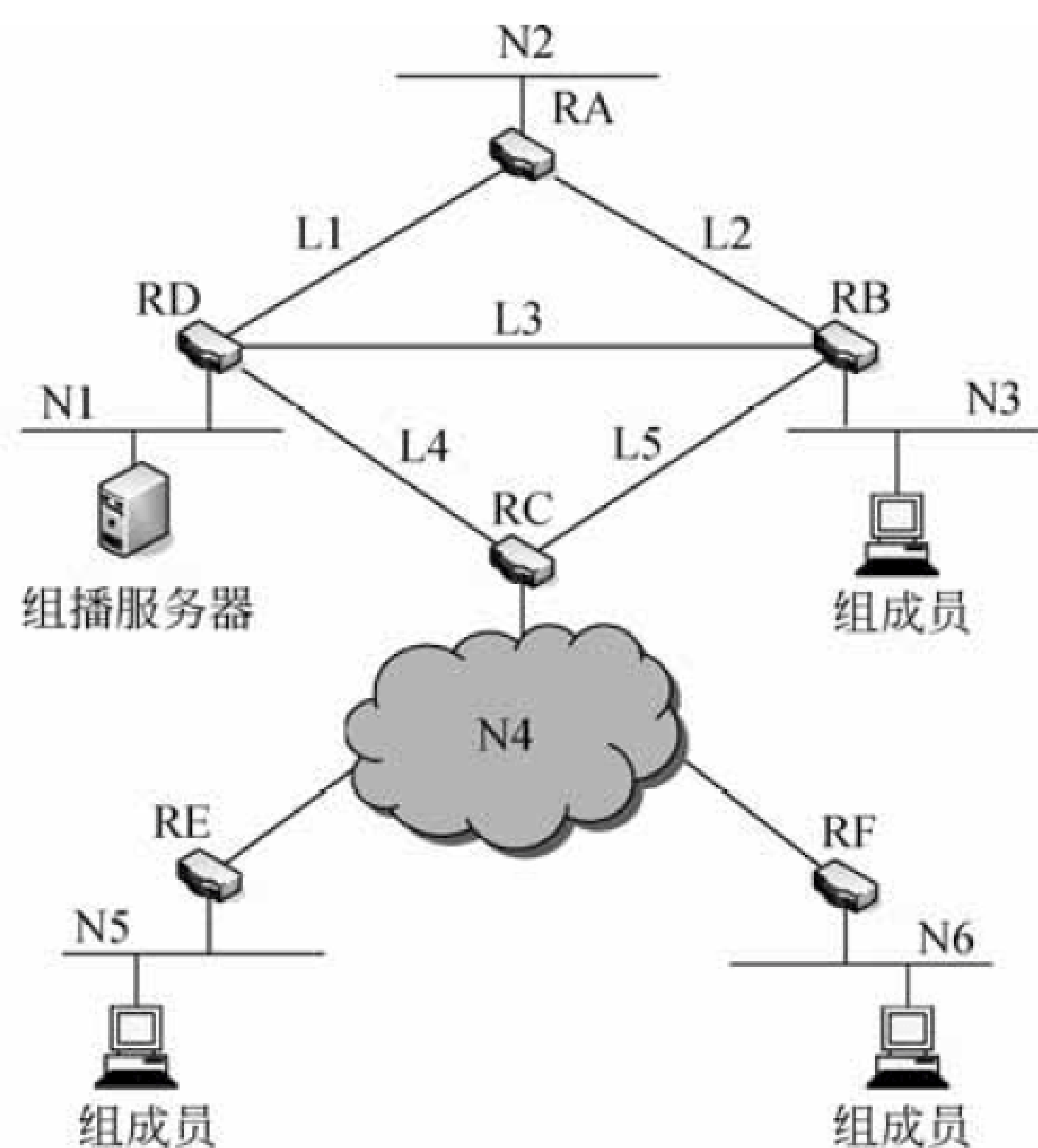
（20）A．包含所有路由器的树
　　B．包含所有组播源的树

C．以组播源为根的最小生成树

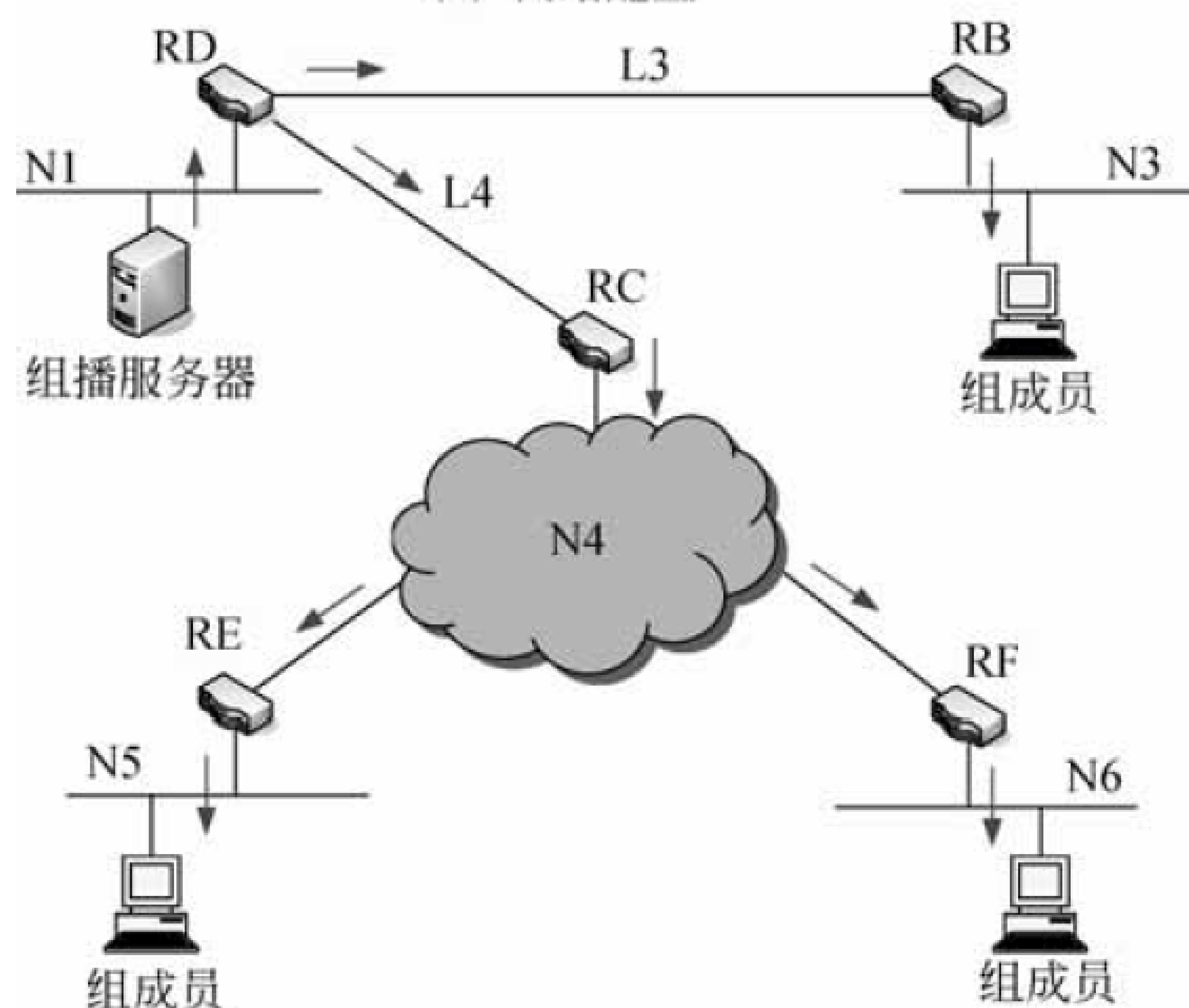
D．以组播路由器为根的最小生成树

**试题（20）分析**

组播树是以组播源为树根的最小生成树（Spanning Tree），沿着这个树从根到叶的方向可以把组播分组传输到所有组成员用户，而分组在每段链路上只出现一次，如下图所示。




（a）网络配置




（b）对应的组播树

建立组播树要使用组播路由协议。组播地址标识一个会话，组播路由器应该互相交换有关组播会话的信息，使得各个路由器了解组播成员的分布情况。对于一个具体的组播会话，即使路由器没有任何成员，但它也需要知道哪些路由器连接着该会话的成员。

如果路由器加入了组播树，那么它就应该知道，在它的哪个端口上存在哪个组的成员，并为之生成相应的组播分支。当一个组成员加入或离开组播会话时，要对组播分支进行嫁接或修剪。

所谓源专用树（Source-Specific Tree）是以每一个组播源为根建立最小生成树，这种树也叫作最短通路树（Shortest Path Tree，SPT）。在组播树中使用了一种称为反向通路转发（Reverse Path Forwarding，RPF）的技术来防止组播分组在网络中循环转发。按照 RPF 规则，在接收到由源 S 向组 G 发送的组播报文后，路由器必须（利用单播路由表）对分组来到的链路进行判断，如果分组来到的链路是通向组播源的最短通路（称为 RPF 通路），则这个分组就被转发到属于分布树的其他端口；如果分组来到的链路不是通向源的最短通路，则分组被抛弃。

还有一种组播树是共享分布树。这种方案利用了由一个（或多个）路由器组成的分布中心来生成一颗组播树，由这棵树负责所有组播组的通信。这种树也称为约会点树（Rendezvous Point Tree，RPT），无论哪个组播源发送的数据，都先要约会到这一点，然后再沿着共享分布树流向各个接收者。需要接收组播通信流的主机都必须加入共享分布树。

**参考答案**

（20）C

**试题（21）**

资源预约协议（RSVP）用在 IETF 定义的集成服务（IntServv）中建立端到端的 QoS 保障机制。下面关于 RSVP 进行资源预约过程的叙述中，正确的是__（21）__。

（21）A. 从目标到源单向预约

B. 从源到目标单向预约

C. 只适用于点到点的通信环境

D. 只适用于点到多点的通信环境

**试题（21）分析**

IntServ 主要解决的问题是在发生拥塞时如何共享可用的网络带宽，为保证服务质量提供必要的支持。IntServ 通过 4 种手段来提供 QoS 传输机制。

① 准入控制。IntServ 对一个新的 QoS 通信流要进行资源预约。如果网络中的路由器确定没有足够的资源来保证所请求的 QoS，则这个通信流就不会进入网络。

② 路由选择算法。可以基于许多不同的 QoS 参数（而不仅仅是最小时延）来进行路由选择。

③ 排队规则。考虑不同通信流的不同需求而采用有效的排队规则。

④ 丢弃策略。在缓冲区耗尽而新的分组来到时要决定丢弃哪些分组以支持 QoS 传输。

为了实现 QoS 传输，必须对现有的路由器进行改造，使其在传统的存储—转发功能

之外，还能够提供资源预约、准入控制、队列管理以及分组调度等高级功能。

- 资源预约协议（Resource Reservation Protocol，RSVP）：按照通信流的 QoS 需求在网络中传送资源预约信令。RSVP 要把带宽、时延、抖动和丢包率等参数通知通路上的所有转发设备，以便建立端到端的 QoS 保障。如果通信流的 QoS 请求得到满足，则 RSVP 还要更新路由器中的数据库，以便及时反映网络通信资源的分配情况。RSVP 是从源到目标单向预约的，适用于点到点以及点到多点的通信环境。
- 准入控制（Admission Control）：当一个新的通信流成功地实现资源预约后就进入通信阶段，这时路由器要监视通信流的行为是否违反了网络与用户达成的合约，以决定是否允许新的分组进入网络。
- 管理代理：其作用是修改通信控制数据库，以改变准入控制的策略。
- 分类器（Classifier）：根据预置的规则对进入路由器的分组进行分类。分类的标准可能是源地址、目标地址、上层协议类型、源端口号和目标端口号等。分组经过分类以后进入不同的队列等待调度器的转发服务。
- 分组调度器（Scheduler）：其作用是根据预订的调度算法对分类后的分组进行排队，可以使用先来先服务的算法，或者更复杂的“公平”算法。例如，WFQ（Weighted Fair Queueing）算法考虑了每个通信流的分组数量，越忙的队列分配越多的容量，而又不完全关闭流量偏少的队列。调度器根据分组的类别、通信控制数据库的内容以及输出端口的活动历史选择被丢弃的分组，决定分组被转发的优先顺序。

**参考答案**

（21）B

**试题（22）、（23）**

为了解决伴随 RIP 协议的路由环路问题，可以采用水平分割法，这种方法的核心是 （22） ，而反向毒化方法则是 （23） 。

（22）A．把网络水平地分割为多个网段，网段之间通过指定路由器发布路由信息
B．一条路由信息不要发送给该信息的来源
C．把从邻居学习到的路由费用设置为无限大并立即发送给那个邻居
D．出现路由变化时立即向邻居发送路由更新报文

（23）A．把网络水平地分割为多个网段，网段之间通过指定路由器发布路由信息
B．一条路由信息不要发送给该信息的来源
C．把从邻居学习到的路由费用设置为无限大并立即发送给那个邻居
D．出现路由变化时立即向邻居发送路由更新报文

**试题（22）、（23）分析**

距离矢量法算法要求相邻的路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换的过程如果不加以限制，将会形成路

由环路（Routing Loops），使得各个路由器无法就网络的可到达性取得一致。

解决路由环路问题可以采用水平分割法（Split Horizon）。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。

简单的水平分割方案是："不能把从邻居学习到的路由发送给那个邻居"，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse）是："把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居"。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

**参考答案**

（22）B　（23）C

**试题（24）**

OSPF 网络被划分为各种区域，其中作为区域之间交换路由信息的是＿（24）＿。

（24）A．主干区域　　B．标准区域
　　C．存根区域　　D．不完全存根区域

**试题（24）分析**

每个 OSPF 区域被指定了一个 32 位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为 0.0.0.0。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

- 标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。
- 主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。
- 存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由 0.0.0.0。
- 完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的，是非标准的。
- 不完全存根区域（NSAA）：类似于存根区域，但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

**参考答案**

（24）A

**试题（25）、（26）**

OSPF 将路由器连接的物理网络划分为以下 4 种类型，以太网属于＿（25）＿，X.25 分组交换网属于＿（26）＿。

（25）A．点对点网络　　B．广播多址网络

C．点到多点网络　　D．非广播多址网络

（26）A．点对点网络　　B．广播多址网络

C．点到多点网络　　D．非广播多址网络

**试题（25）、（26）分析**

网络的物理连接和拓扑结构不同，交换路由信息的方式就不同。OSPF 将路由器连接的物理网络划分为 4 种类型：

- 点对点网络：例如一对路由器用 64kb 的串行线路连接，就属于点对点网络，在这种网络中，两个路由器可以直接交换路由信息。
- 广播多址网络：以太网或者其他具有共享介质的局域网都属于这种网络。在这种网络中，一条路由信息可以广播给所有的路由器。
- 非广播多址网络（non-broadcast multi-access，NBMA）：例如 X.25 分组交换网就属于这种网络，在这种网络中可以通过组播方式发布路由信息。
- 点到多点网络：可以把非广播网络当作多条点对点网络来使用，从而把一条路由信息发送到不同的目标。

**参考答案**

（25）B　（26）D

**试题（27）**

采用 DHCP 动态分配 IP 地址，如果某主机开机后没有得到 DHCP 服务器的响应，则该主机获取的 IP 地址属于网络 （27） 。

（27）A．192.168.1.0/24　　B．172.16.0.0/24

C．202.117.0.0/16　　D．169.254.0.0/16

**试题（27）分析**

如果运行 Windows 的计算机没有配置静态地址，并且也无法从 DHCP 服务器中获取动态地址，那么它将在网络 169.254.0.0/16 中随机选取一个自动专用 IP 地址（APIPA）。在 RFC 3330 和 RFC 3927 中，把这种地址称作 IPv4 链路本地（IPv4 LL）地址或零配置网络。

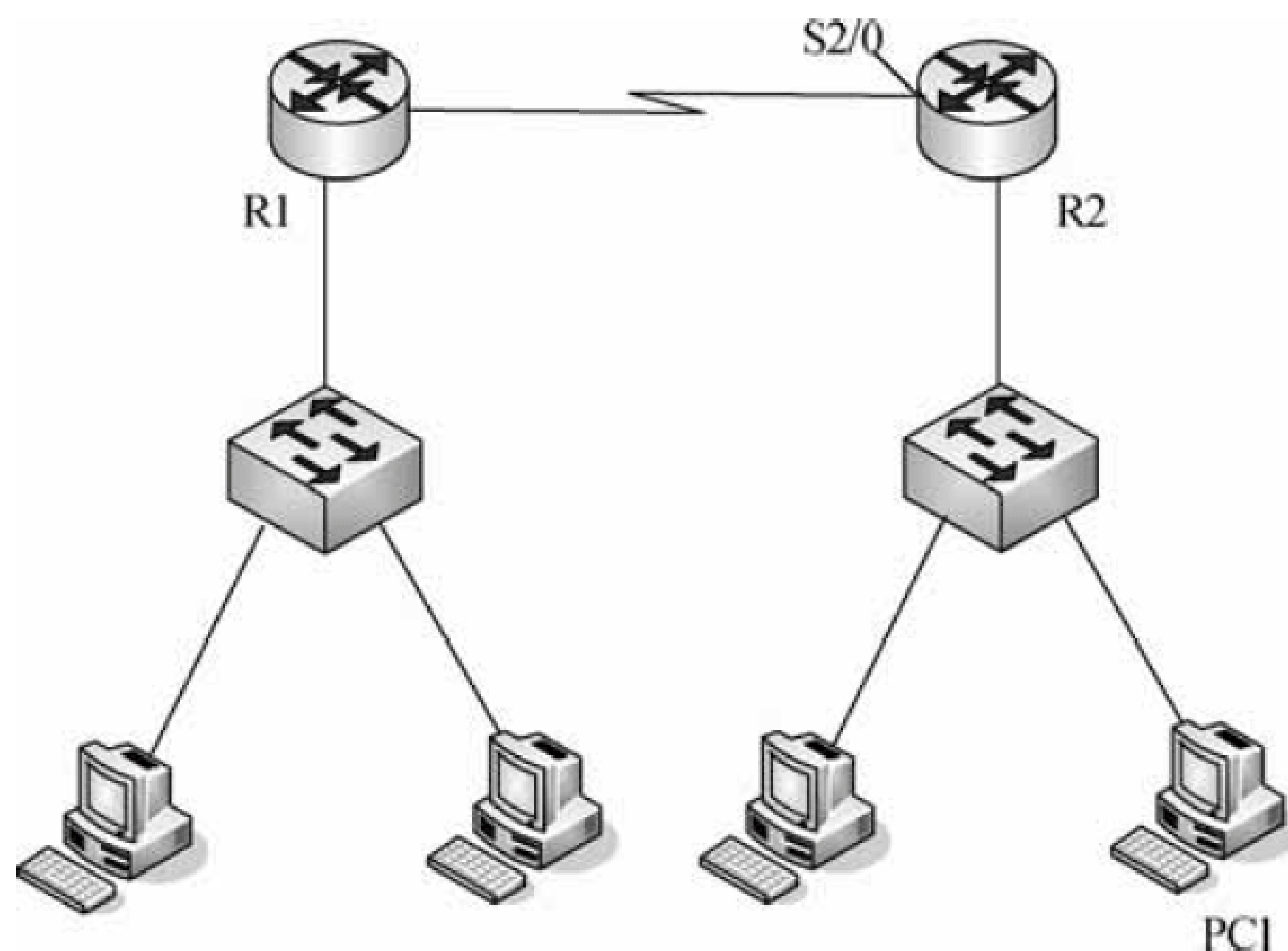
APIPA 使得在 Ad-hoc 无线局域网中的计算机无须配置 DHCP 服务器或静态 IP 地址而可以互相通信。如果在提供有 DHCP 服务器的网络上计算机的 IP 地址是 APIPA，这就意味着该计算机无法联系上 DHCP 服务器。该计算机可能没有正确接入网络或是 DHCP 服务器掉线。

**参考答案**

（27）D

**试题（28）～（31）**

某网络拓扑结构如下图所示。




在路由器 R2 上采用命令（28）得到如下图所示结果。PC1 可能的 IP 地址为（29），路由器 R2 的 S0 口的 IP 地址为（30）。若在 PC1 上查看主机的路由表，采用的命令为（31）。

```
R2>
…
R    192.168.0.0/24 [120/1] via 202.117.112.1, 00:00:11, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
   202.117.112.0/30 is subnetted, 1 subnets
C    202.117.112.0 is directly connected, Serial2/0
R2>
```

（28）A. nslookup　B. route print　C. ip routing　D. show ip route
（29）A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2
（30）A. 192.168.0.1　B. 192.168.1.1　C. 202.117.112.1　D. 202.117.112.2
（31）A. nslookup　B. route print　C. ip routing　D. show ip route

**试题（28）～（31）分析**

本试题考查 RIP 协议及路由信息相关内容。

路由器上查看路由协议的命令为 show ip route。

从路由器 R2 的命令看出：网络 192.168.1.0/24 与 R2 直连，202.117.112.0 与 R2 直连，192.168.0.0/24 不是直接连接，是路由器采用 RIP 协议进行转发的。PC1 与路由器直连，又 202.117.112.1 是路由器的接口，故 PC1 属于网络 192.168.1.0/24，只可能是 192.168.1.1。

202.117.112.1 是路由器 R2 到网络 192.168.0.0/24 的下一条，即路由器 R1 上与 R2 连接的接口，故路由器 R2 的 S0 口的 IP 地址为 202.117.112.2。

在主机上查看主机的路由表的命令为 route print 或 netstat -r。

**参考答案**

（28）D　（29）B　（30）D　（31）B

**试题（32）～（34）**

DNS 反向搜索功能的作用是（32），资源记录 MX 的作用是（33），DNS 资源记录（34）定义了区域的反向搜索。

（32）A．定义域名服务器的别名
B．将 IP 地址解析为域名
C．定义域邮件服务器地址和优先级
D．定义区域的授权服务器

（33）A．定义域名服务器的别名
B．将 IP 地址解析为域名
C．定义域邮件服务器地址和优先级
D．定义区域的授权服务器

（34）A．SOA　B．NS　C．PTR　D．MX

**试题（32）～（34）分析**

DNS 正向搜索功能的作用是将域名解析为 IP 地址，反向搜索功能的作用是将 IP 地址解析为域名。资源记录 MX 的作用是定义域邮件服务器地址和优先级。定义了区域的反向搜索的是 DNS 资源记录 PTR。

**参考答案**

（32）B　（33）C　（34）C

**试题（35）**

在 Linux 系统中，使用 Apache 服务器时默认的 Web 根目录是（35）。

（35）A．..\htdocs　B．/var/www/html
C．/var/www/usage　D．..\conf

**试题（35）分析**

本题考查 Apache 服务器方面的基础知识。

Apache 是常见的 Web 服务器之一，在安装目录下，有\bin、\conf、\var/www/html、/var/www/usage 等目录。其中，\bin 目录中存放的是 DLL 文件，\conf 目录中存放服务器的配置文件等，/var/www/html 目录中存放的是 Web 服务器网站文件，/var/www/usage 目录中存放用户文件，\htdocs 目录是 Windows 下 Apache 的 Web 文件存放目录。

**参考答案**

（35）B

**试题（36）**

下面关于 Linux 系统文件挂载的叙述中，正确的是（36）。

（36）A．/可以作为一个挂载点
B．挂载点可以是一个目录，也可以是一个文件
C．不能对一个磁盘分区进行挂载

D．挂载点是一个目录时，这个目录必须为空

**试题（36）分析**

本题考查 Linux 操作系统方面的基础知识。

在 Linux 系统中，挂载点必须是一个目录，一个分区可以挂载在一个已存在的目录上，这个目录可以不为空，但挂载后这个目录下以前的内容将不可用。

**参考答案**

（36）A

**试题（37）**

在浏览器的地址栏中输入 xxxyftp.abc.com.cn，该 URL 中__（37）__是要访问的主机名。

（37）A．xxxyftp　　B．abc　　C．com　　D．cn

**试题（37）分析**

本题考查 URL 方面的基础知识。

一个 URL 通常由“协议名”“://”“主机名”“.”“域名”“/”“目录名”“/”“文件名”构成。题目中所给的 URL 不包含协议名称，按照以上描述，要访问的主机名为 xxxyftp，该字段后面的 abc.com.cn 属于域名。

**参考答案**

（37）A

**试题（38）**

下列关于 DHCP 服务的叙述中，正确的是__（38）__。

（38）A．一台 DHCP 服务器只能为其所在网段的主机分配 IP 地址

B．对于移动用户设置较长的租约时间

C．DHCP 服务器不需要配置固定的 IP 地址

D．在 Windows 客户机上可使用 ipconfig /release 释放当前 IP 地址

**试题（38）分析**

本题考查 DHCP 基础知识。

DHCP 服务器用于为网络中的客户端自动分配 IP 地址配置信息，在一个网络中，为了便于管理，只需设置一台 DHCP 服务器。通过 DHCP 中继功能，即可以为多个网段内的主机分配 IP 地址，为了能最大效率使用 IP 地址资源，一般会给 IP 地址使用设置一定的租约期限，常见的设置为 24 小时或者更长的时间，移动用户的 IP 地址分配租期一般设置相对较短。在 Windows 客户机上，ipconfig 命令用于显示当前的 IP 地址配置信息，若加上/release 参数，则可将当前的 IP 地址配置释放掉，以便于重新申请 IP 地址配置信息。

**参考答案**

（38）D

**试题（39）、（40）**

当接收邮件时，客户端与 POP3 服务器之间通过__（39）__建立连接，所使用的端口是__（40）__。

（39）A. UDP　　B. TCP　　C. HTTP　　D. HTTPS

（40）A. 25　　B. 52　　C. 1100　　D. 110

**试题（39）、（40）分析**

本题考查邮件服务方面的基础知识。

邮件服务是互联网的主要服务之一，其使用 SMTP 和 POP3 两种协议，其中 SMTP 协议用于发送电子邮件，使用 25 号端口，POP3 协议用于接收电子邮件，使用 110 号端口。这两种协议均是基于面向连接的 TCP 协议的应用层协议。

**参考答案**

（39）B　（40）D

**试题（41）～（43）**

用户 B 收到经 A 数字签名后的消息 M，为验证消息的真实性，首先需要从 CA 获取用户 A 的数字证书，该数字证书中包含__（41）__，可以利用__（42）__验证该证书的真伪，然后利用__（43）__验证 M 的真实性。

（41）A. A 的公钥　　B. A 的私钥
　　C. B 的公钥　　D. B 的私钥

（42）A. CA 的公钥　　B. B 的私钥
　　C. A 的公钥　　D. B 的公钥

（43）A. CA 的公钥　　B. B 的私钥
　　C. A 的公钥　　D. B 的公钥

**试题（41）～（43）分析**

本题考查数字签名和 CA 方面的基础知识。

CA 是认证中心的简称，为了能够在互联网上认证通信双方的身份，可以在相应的认证中心申请自己的数字证书。CA 为用户颁发的数字证书中包含用户的公钥信息、权威机构的认证信息和有效期等。用户收到经数字签名的消息后，须首先验证证书的真伪，即使用证书的公钥来验证，然后利用对方的公钥来验证消息的真实性。

**参考答案**

（41）A　（42）A　（43）C

**试题（44）**

3DES 的密钥长度为__（44）__。

（44）A. 56　　B. 112　　C. 128　　D. 168

**试题（44）分析**

本题考查 DES 加密算法方面的基础知识。

DES 加密算法使用 56 位的密钥以及附加的 8 位奇偶校验位（每组的第 8 位作为奇偶校验位），产生最大 64 位的分组大小。这是一个迭代的分组密码，将加密的文本块分成两半。使用子密钥对其中一半应用循环功能，然后将输出与另一半进行“异或”运算；接着交换这两半，这一过程会继续下去，但最后一个循环不交换。DES 使用 16 轮循环，使用异或，置换，代换，移位操作四种基本运算。三重 DES 所使用的加密密钥长度为 112 位。

**参考答案**

（44）B

**试题（45）**

下列不属于报文认证算法的是__（45）__。

（45）A．MD5　　B．SHA-1　　C．RC4　　D．HMAC

**试题（45）分析**

本题考查报文认证算法方面的基础知识。

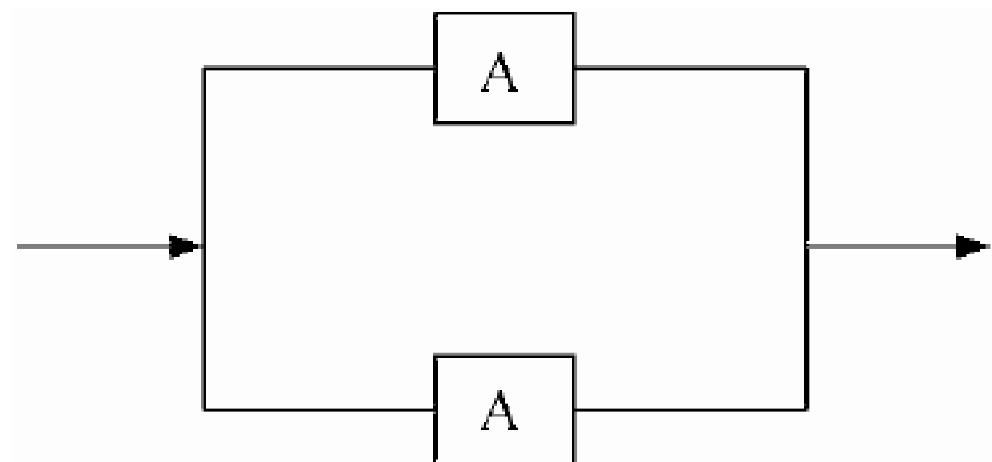
报文认证是为了防止可能对网络中传输的数据存在的伪装回放、顺序修改、计时修改等攻击所采用的保护措施，一般采用消息认证或数字签名的方式来对报文进行进一步的保护。通过认证，可以使得消息的接收者确认消息确实来自真正的发送者，同时确认消息内容没有被修改，可以验证消息的顺序和及时性。一般采用的算法有：MD5、SHA-1、HMAC 几种算法。RC4 算法是一种加密算法。

**参考答案**

（45）C

**试题（46）**

设备 A 的可用性为 0.98，如下图所示将设备 A 并联以后的可用性为__（46）__。




（46）A．0.9604　　B．0.9800　　C．0.9996　　D．0.9999

**试题（46）分析**

由于网络系统由许多网络元素组成，所以系统的可靠性不但与各个元素的可靠性有关，而且还与网络元素的组织形式有关。根据一般可靠性理论，若两个元素串联，则可用性减少。例如两个 Modem 串联在链路的两端，若单个 Modem 的可用性 A=0.98，并假定链路其他部分的可用性为 1，则整个链路的可用性 A=0.98×0.98=0.9604；若两个元素并联，则可用性增加。例如终端通过两条链路连接到主机，若一条链路失效，另外一条链路自动备份。假定单个链路的可用性 A=0.98，则双链路的可用性

$$A=2\times0.98-0.98\times0.98=1.96-0.9604=0.9996$$

**参考答案**

（46）C

**试题（47）**

SNMP 采用 UDP 提供的数据报服务，这是由于＿（47）＿。

（47）A．UDP 比 TCP 更加可靠

B．UDP 报文可以比 TCP 报文大

C．UDP 是面向连接的传输方式

D．采用 UDP 实现网络管理不会太多增加网络负载

**试题（47）分析**

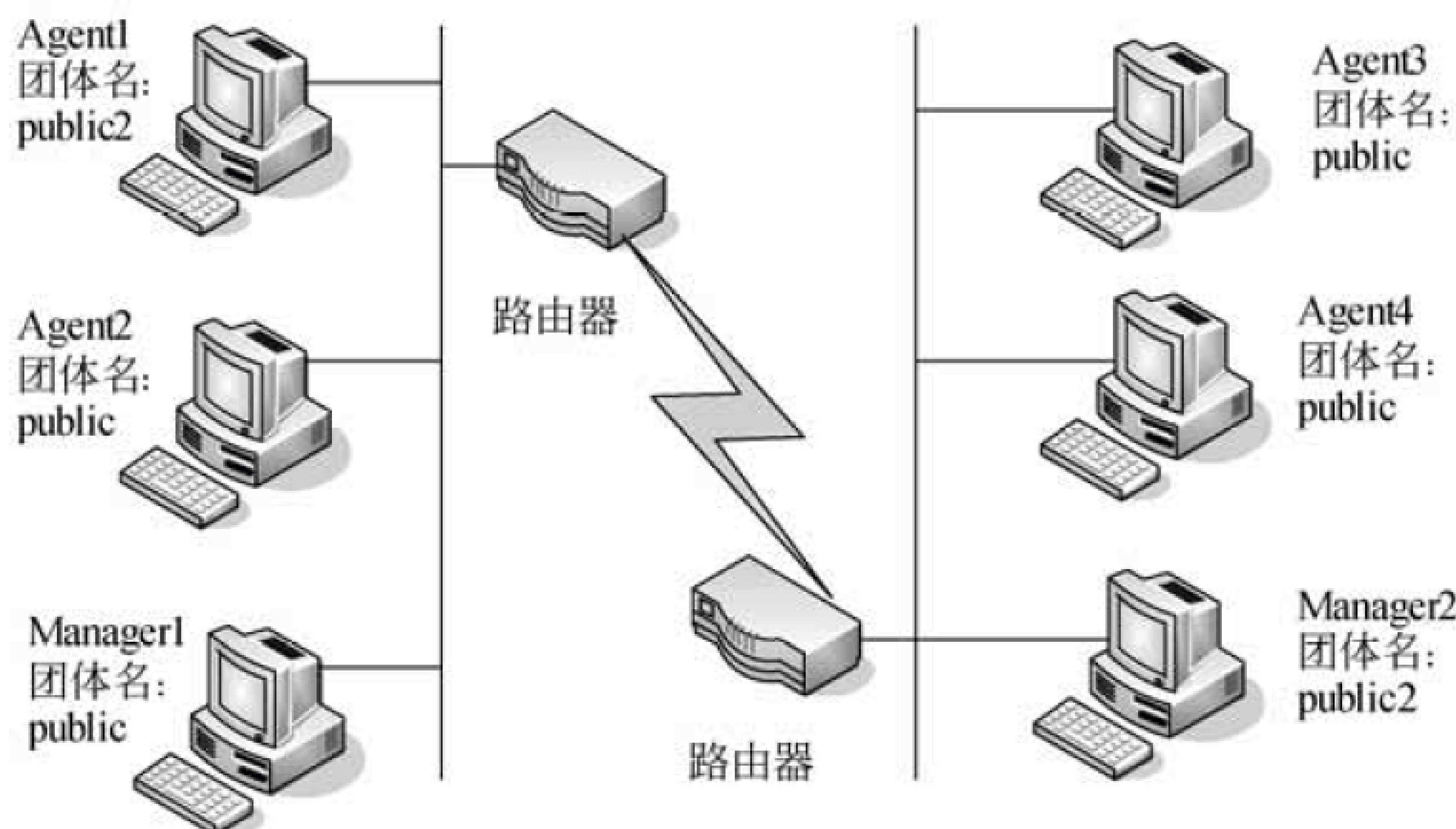
由于 SNMP 为应用层协议，所以它依赖于 UDP 数据报服务。同时 SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。其所以选择 UDP 协议而不是 TCP 协议，这是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不是很可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现的建议是，对每个管理信息要装配成单独的数据报独立发送，而且报文应短些，不要超过 484 字节。

**参考答案**

（47）D

**试题（48）**

在下图的 SNMP 配置中，能够响应 Manager2 的 getRequest 请求的是＿（48）＿。




（48）A．Agent1　　B．Agent2　　C．Agent3　　D．Agent4

**试题（48）分析**

在 SNMP 管理中，管理站和代理之间进行信息交换时要通过团体名认证，这是一种简单的安全机制，管理站与代理必须具有相同的团体名才能互相通信。但是由于包含团

体名的 SNMP 报文是明文传送，所以这样的认证机制是不够安全的。本题中的 Manager2 和 Agent1 的团体名都是 public2，所以二者可以互相通信。

**参考答案**

（48）A

**试题（49）**

客户端采用 ping 命令检测网络连接故障时，可以 ping 通 127.0.0.1 及本机的 IP 地址，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址。该客户端的故障可能是<u>（49）</u>。

（49）A．TCP/IP 协议不能正常工作　　B．本机网卡不能正常工作
　　　C．网络线路故障　　　　　　　D．本机 DNS 服务器地址设置错误

**试题（49）分析**

客户端可以 ping 通 127.0.0.1 及本机的 IP 地址，说明 TCP/IP 协议工作正常，并且本机的网卡也工作正常，但无法 ping 通同一网段内其他工作正常的计算机的 IP 地址，故可以考虑是网络线路故障。由于该检测 ping 的都是 IP 地址，所以与 DNS 服务器无关。

**参考答案**

（49）C

**试题（50）**

在 Windows 的 DoS 窗口中输入命令

```
C:\> nslookup
> set type=ptr
> 211.151.91.165
```

这个命令序列的作用是<u>（50）</u>。

（50）A．查询 211.151.91.165 的邮件服务器信息
　　　B．查询 211.151.91.165 到域名的映射
　　　C．查询 211.151.91.165 的资源记录类型
　　　D．显示 211.151.91.165 中各种可用的信息资源记录

**试题（50）分析**

Nslookup 命令用于显示 DNS 查询信息，诊断和排除 DNS 故障。Nslookup 有交互式和非交互式两种工作方式。在交互式工作方式下输入> set type=ptr 表示由地址查询域名，所以本题中命令序列的作用是查询地址 211.151.91.165 到域名的映射。

**参考答案**

（50）B

**试题（51）**

下面 4 个主机地址中属于网络 220.115.200.0/21 的地址是<u>（51）</u>。

（51）A．220.115.198.0　　　　B．220.115.206.0
　　　C．220.115.217.0　　　　D．220.115.224.0

**试题（51）分析**

地址 220.115.198.0 的二进制形式是　1101 1100．0111 0011．1100 0110．0000 0000

地址 220.115.206.0 的二进制形式是　**1101 1100．0111 0011．1100 1**110．0000 0000

地址 220.115.217.0 的二进制形式是　1101 1100．0111 0011．1101 1001．0000 0000

地址 220.115.224.0 的二进制形式是　1101 1100．0111 0011．1110 0000．0000 0000

而地址 220.115.200.0/21 的二进制形式是 **1101 1100．0111 0011．1100 1**000．0000 0000

所以与地址 220.115.200.0/21 匹配的是 220.115.206.0。

**参考答案**

（51）B

**试题（52）、（53）**

假设路由表有 4 个表项如下所示，那么与地址 115.120.145.67 匹配的表项是__（52）__，与地址 115.120.179.92 匹配的表项是__（53）__。

（52）A.115.120.145.32　　　　B.115.120.145.64
　　　C.115.120.147.64　　　　D.115.120.177.64

（53）A.115.120.145.32　　　　B.115.120.145.64
　　　C.115.120.147.64　　　　D.115.120.177.64

**试题（52）、（53）分析**

地址 115.120.145.32 的二进制形式是 0111 0011．0111 1000．1001 0001．0010 0000

地址 115.120.145.64 的二进制形式是 0111 0011．0111 1000．1001 0001．0100 0000

地址 115.120.147.64 的二进制形式是 0111 0011．0111 1000．1001 0011．0100 0000

地址 115.120.177.64 的二进制形式是 0111 0011．0111 1000．1011 0001．0100 0000

地址 115.120.145.67 的二进制形式是 0111 0011．0111 1000．1001 0001．0100 0011

按照最长匹配规则，地址 115.120.145.67 与 115.120.145.64 匹配。

地址 115.120.179.92 的二进制形式是 0111 0011．0111 1000．1011 0011．0101 1100

按照最长匹配规则，地址 115.120.179.92 与 115.120.177.64 匹配。

**参考答案**

（52）B　（53）D

**试题（54）、（55）**

假设分配给用户 U1 的网络号为 192.25.16.0～192.25.31.0，则 U1 的地址掩码应该为__（54）__；假设分配给用户 U2 的网络号为 192.25.64.0/20，如果路由器收到一个目标地址为 11000000.00011001.01000011.00100001 的数据报，则该数据报应传送给用户__（55）__。

（54）A．255.255.255.0　　　　B．255.255.250.0
　　　C．255.255.248.0　　　　D．255.255.240.0

（55）A．U1　　B．U2　　C．U1 或 U2　　D．不可到达

**试题（54）、（55）分析**

用户 U1 的网络号为 192.25.16.0～192.25.31.0，包含 16 个 C 类网络，则 U1 的地址掩码应该为 255.255.240.0；路由器收到的数据报的目标地址为 192.25.67.33（由二进制形式翻译的），显然该数据报应传送给用户 U2。

**参考答案**

（54）D　（55）B

**试题（56）**

路由器 Console 端口默认的数据速率为__（56）__。

（56）A．2400b/s　　B．4800b/s　　C．9600b/s　　D．10Mb/s

**试题（56）分析**

路由器 Console 端口默认的数据速率为 9600b/s，如下图所示。




**参考答案**

（56）C

**试题（57）**

路由器命令 R1(config) # ip routing 的作用是__（57）__。

（57）A．显示路由信息　　B．配置默认路由

C．激活路由器端口　　D．启动路由配置

**试题（57）分析**

路由器命令 ip routing 的作用是启动路由配置，no ip routing 的作用是关闭 ip 路由配置。

**参考答案**

（57）D

**试题（58）**

在路由器的特权模式下输入命令 setup，则路由器进入__（58）__。

（58）A．用户命令状态　　B．局部配置状态

C．特权命令状态　　D．设置对话状态

**试题（58）分析**

在特权命令状态下使用 setup 命令可进入对话状态，这是一台新路由器开机时自动进入的状态。在这种状态下用户可以通过“yes”或者“no”选择是否使用设置对话方式对路由器进行管理和配置。

**参考答案**

（58）D

**试题（59）**

使用 IEEE 802.1q 协议，最多可以配置__（59）__个 VLAN。

（59）A．1022　　B．1024　　C．4094　　D．4096

**试题（59）分析**

IEEE 802.1q 定义了 VLAN 帧标记的格式，如下图所示。可以看出 VID 字段为 12 位，可表示的 VLAN 标识符为 0～4095，其中 VID 0 用于识别优先级，VID 4095 保留未用，所以最多可配置 4094 个 VLAN。

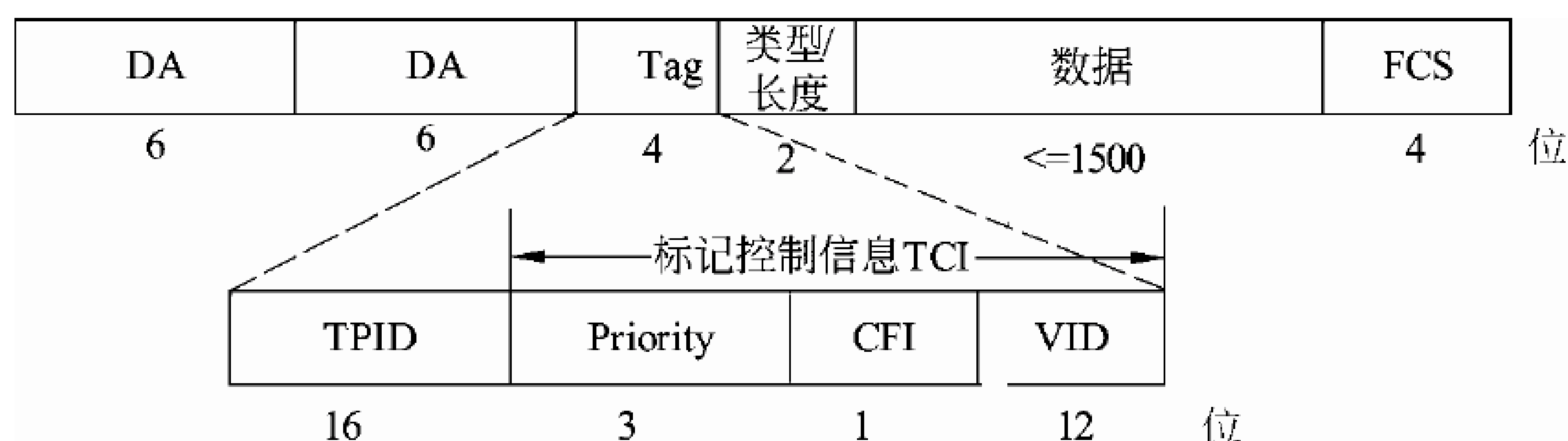



图　802.1q 帧格式

**参考答案**

（59）C

**试题（60）**

VLAN 中继协议（VTP）有不同的工作模式，其中能够对交换机的 VLAN 信息进行添加、删除、修改等操作，并把配置信息广播到其他交换机上的工作模式是__（60）__。

（60）A．客户机模式　　B．服务器模式

C．透明模式　　D．控制模式

**试题（60）分析**

管理员可以使用 VTP 协议为交换机设置 VLAN。VTP 有三种工作模式，即服务器模式（Server Mode）、客户模式（Client Mode）和透明模式（Transparent Mode）。这三

种模式的区别如下：

- 服务器模式：处于该模式下，管理员可以对交换机上的 VLAN 信息进行添加、删除、修改等操作，并且交换机会将这些信息自动广播到与其连接的其他交换机上，用以统一 VLAN 配置。
- 客户模式：处于该模式下，管理员不能对交换机上的 VLAN 信息进行任何操作，交换机只能接受服务器模式的交换机所广播的 VLAN 配置信息，并将其应用到本地。
- 透明模式：处于该模式下的交换机，管理员可以对交换机上的 VLAN 信息进行添加、删除和修改等操作，但这些配置信息并不对其他交换机广播，不会将服务器模式下的交换机所发送的配置信息应用到本地，而是直接转发。

交换机的初始状态是工作在服务器模式，有一个默认的 VLAN（VLAN 1），所有的端口都属于这个 VLAN。

**参考答案**

（60）B

**试题（61）**

下面关于 VTP 修剪的论述中，错误的是＿（61）＿。

（61）A．静态修剪就是手工剪掉中继链路上不活动的 VLAN
B．动态修剪使得中继链路上所有共享的 VLAN 都是活动的
C．静态修剪要求在 VTP 域中的所有交换机都配置成客户机模式
D．动态修剪要求在 VTP 域中的所有交换机都配置成服务器模式

**试题（61）分析**

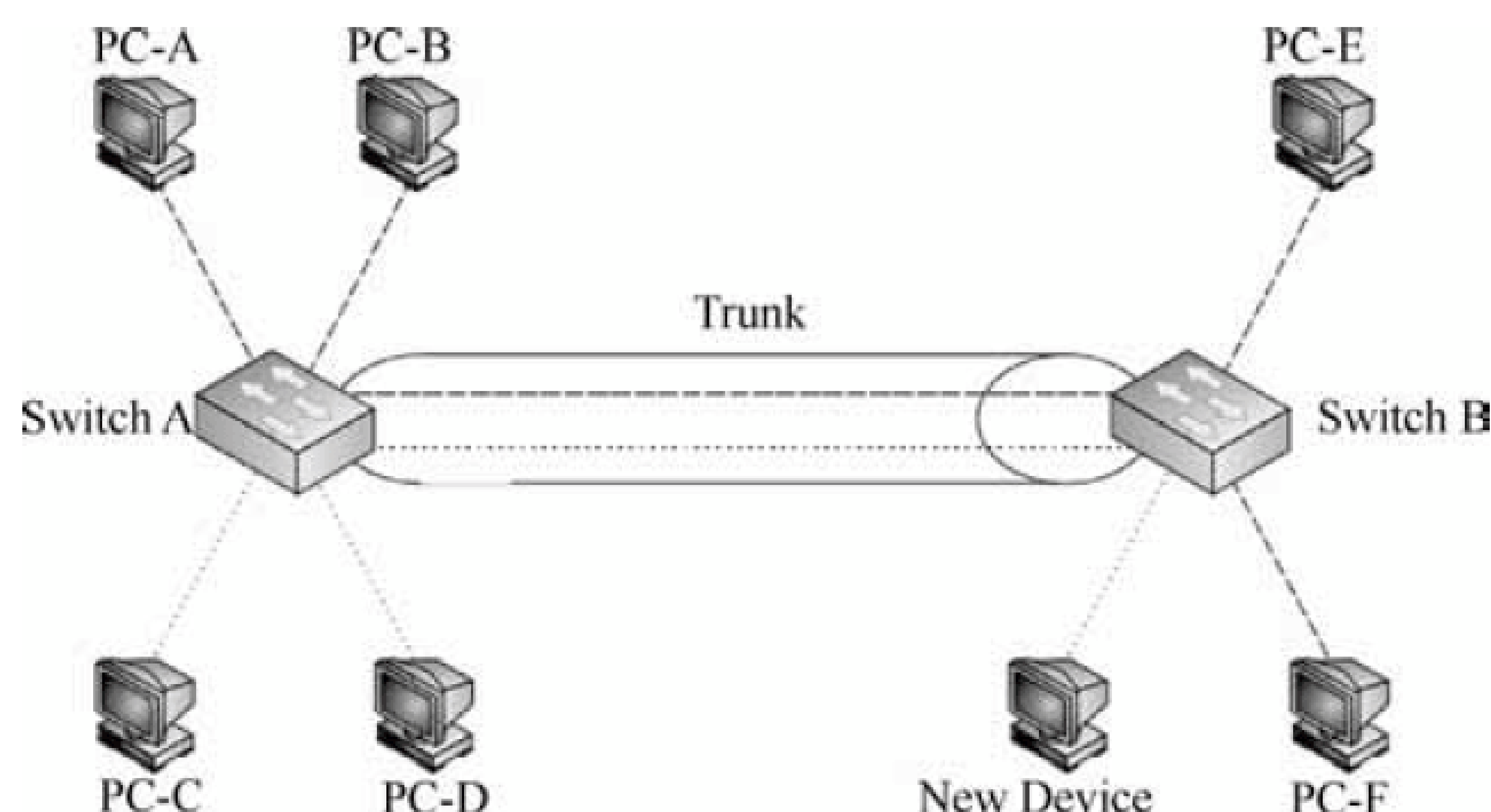
在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛（flood）到所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪会遇到一些问题，如果后来在交换机上又添加了活动 VLAN 的成员，则必须重新改变交换机的配置。在多个交换机组成多个 VLAN 的网络中，这种工作方式容易出错。

VTP 动态修剪允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN1 和 VLAN2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

这样做的好处是显而易见的，如果以后在交换机 B 上添加了 VLAN 2 的成员，交换

机 B 就会通知交换机 A，它有了一个新的活动的 VLAN 2，于是，两个交换机动态地把 VLAN 2 添加到它们之间的中继链路配置中，如下图所示。




VTP 动态修剪的缺点是它要求在 VTP 域中的所有交换机都必须配置成服务器。由于交换机在服务器模式下工作时可以改变 VLAN 配置，也可以接受 VLAN 配置的改变，所以当多个管理员在多个服务器上同时配置 VLAN 时将会出现灾难性的后果。

**参考答案**

（61）C

**试题（62）**

IEEE 802.3ae 10Gb/s 以太网标准支持的工作模式是＿（62）＿。

（62）A. 单工　　B. 半双工

C. 全双工　　D. 全双工和半双工

**试题（62）分析**

2002 年 6 月发布的 IEEE 802.3ae 标准支持 10Gb/s 的传输速率，规定的几种传输介质如下表所示。传统以太网采用 CSMA/CD 协议，即带冲突检测的载波监听多路访问技术。万兆以太网与千兆以太网一样，基本上应用于点到点线路，不再共享带宽，只适用于全双工模式，不需要 CSMA/CD 协议支持。除此之外，万兆以太网与原来的以太网模型完全相同，仍然保留了以太网帧结构，只是通过不同的编码方式或波分复用提供 10Gb/s 传输速度。千兆以太网和万兆以太网采用与传统以太网同样的帧结构。

**表　IEEE 802.3ae 万兆以太网标准**

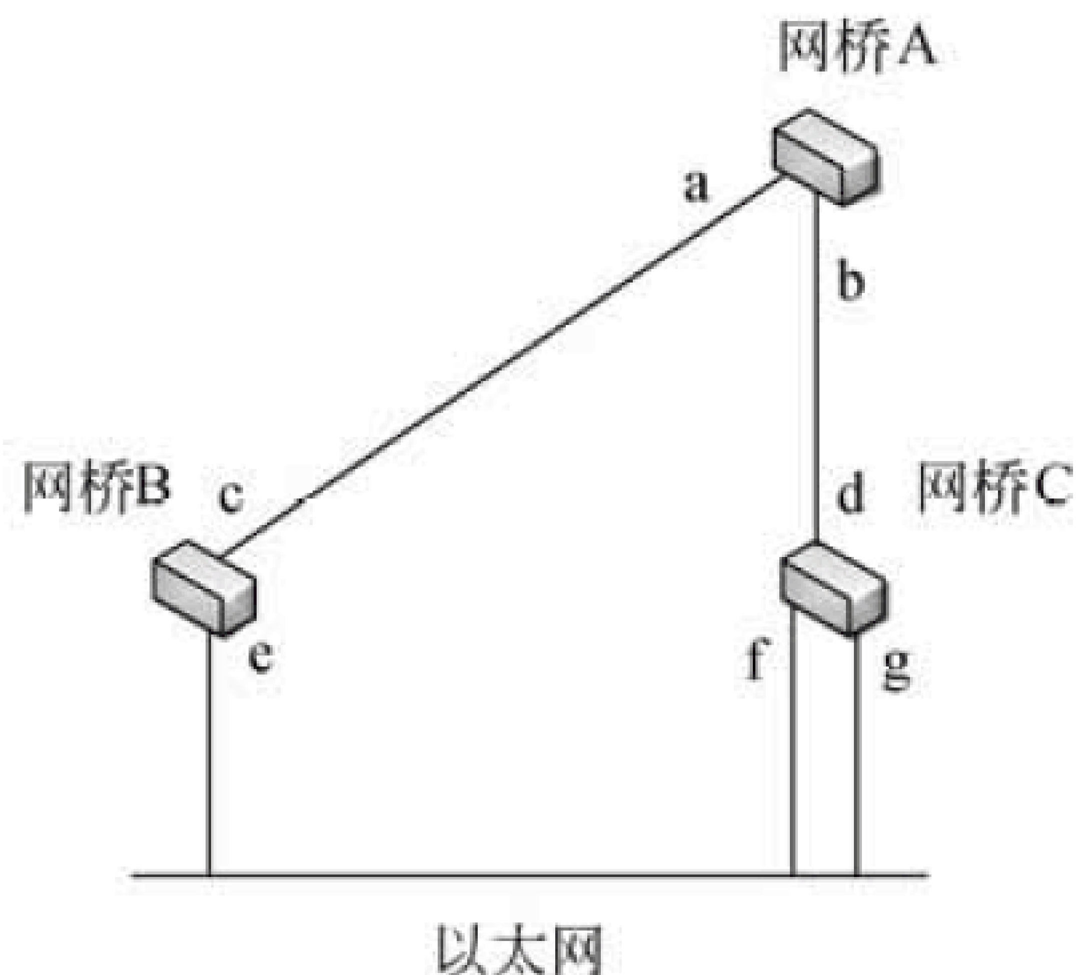
| 名　称 | 电　缆 | 最大段长 | 特　点 |
|---|---|---|---|
| 10GBase-S（Short） | 50μm 的多模光纤 | 300m | 850nm 串行 |
| | 62.5μm 的多模光纤 | 65m | |
| 10GBase-L（Long） | 单模光纤 | 10km | 1310nm 串行 |
| 10GBase-E（Extended） | 单模光纤 | 40km | 1550nm 串行 |
| 10GBase-LX4 | 单模光纤 | 10km | 1310nm<br>4×2.5Gb/s<br>波分多路复用（WDM） |

**参考答案**

（62）C

**试题（63）**

如下图所示，网桥 A、B、C 连接多个以太网。已知网桥 A 为根网桥，各个网桥的 a、b、f 端口为指定端口。那么按照快速生成树协议标准 IEEE 802.1d-2004，网桥 B 的 c 端口为 <u>（63）</u> 。




（63）A．根端口（Root Port）　　B．指定端口（Designated Port）

C．备份端口（Backup Port）　　D．替代端口（Alternate Port）

**试题（63）分析**

由于网桥 A 为根网桥，a、b、f 为指定端口，所以 c、d 端口为根端口（即通向根网桥的端口）。

**参考答案**

（63）A

**试题（64）**

使用 tracert 命令进行网络检测，结果如下图所示，那么本地默认网关地址是 <u>（64）</u> 。

```
C:\>tracert 110.150.0.66
Tracing route to 110.150.0.66 over a maximum of 30 hops
1 2s 3s 2s 10.10.0.1
2 75ms 80ms 100ms 192.168.0.1
3 77ms 87ms 54ms 110.150.0.66
Trace complete
```

（64）A．110.150.0.66　　B．10.10.0.1　　C．192.168.0.1　　D．127.0.0.1

**试题（64）分析**

Tracert 命令的功能是确定到达目标的路径，并显示通路上每一个中间路由器的 IP 地址。通过多次向目标发送 ICMP 回声（echo）请求报文，每次增加 IP 头中 TTL 字段

的值，就可以确定到达各个路由器的时间。显示的地址是路由器接近源的这一边的端口地址。本题中最先遇到的路由器地址是 10.10.0.1，所以这就是本地默认网关的地址。

**参考答案**

（64）B

**试题（65）、（66）**

IEEE 802.11 MAC 子层定义的竞争性访问控制协议是（65），之所以不采用与 IEEE 802.3 相同协议的原因是（66）。

（65）A．CSMA/CA　　B．CSMA/CB
　　　C．CSMA/CD　　D．CSMA/CG

（66）A．IEEE 802.11 协议的效率更高　　B．为了解决隐蔽终端问题
　　　C．IEEE 802.3 协议的开销更大　　D．为了引进多种非竞争业务

**试题（65）、（66）分析**

CSMA/CA 协议类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫作载波监听多路访问/冲突避免协议。在无线网中进行冲突检测是有困难的。例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。

**参考答案**

（65）A　（66）B

**试题（67）**

使用 ADSL 拨号上网，需要在用户端安装（67）协议。

（67）A．PPP　　B．SLIP　　C．PPTP　　D．PPPoE

**试题（67）分析**

ATU-R（ADSL Transceiver Unit-Remote terminal）是 ADSL客户端远程收发单元，通常叫作 ADSL 调制解调器。ATU-R 通过网卡接口连接计算机，在电话线盒一端，引出一条独立电话线连接到分线盒上。分线盒将输入的信号分为低频信号（用于语音通信）和高频信号（用于数据通信）。

通常 PPP 是通过电话线路或 ISDN 线路接驳到 ISP 时使用的。PPPoE（PPP over Ethernet）是在以太网中转播 PPP 帧的技术。PPPoE 协议具有用户认证及通知 IP 地址的功能。在 ADSL 中，PPPoE 用来接驳 ADSL Modem 与个人电脑/家用路由器。

**参考答案**

（67）D

**试题（68）**

在网络中分配 IP 地址可以采用静态地址或动态地址方案。下面关于两种地址分配方案的论述中错误的是（68）。

（68）A．采用动态地址分配方案可避免地址资源的浪费

B．路由器、交换机等连网设备适合采用静态 IP 地址
C．各种服务器设备适合采用动态 IP 地址分配方案
D．学生客户机最好采用动态 IP 地址

**试题（68）分析**

通常采用动态地址分配方案时，把用户计算机和网络中的服务器等设备划分成不同的设备组，给予不同类型的 IP 地址。交换机、路由器、服务器等设备要赋予固定的 IP 地址，以便于用户访问；网络用户则要根据他们使用计算机的特点分配给不同租约期的动态地址，例如移动用户要分配给租约期相对较短的 IP 地址，而办公室用户则要分配给租约期较长的 IP 地址。

**参考答案**

（68）C

**试题（69）、（70）**

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，各个阶段都要产生相应的文档。下面的选项中，属于逻辑网络设计文档的是＿（69）＿，属于物理网络设计文档的是＿（70）＿。

（69）A．网络 IP 地址分配方案　　B．设备列表清单
C．集中访谈的信息资料　　D．网络内部的通信流量分布
（70）A．网络 IP 地址分配方案　　B．设备列表清单
C．集中访谈的信息资料　　D．网络内部的通信流量分布

**试题（69）、（70）分析**

网络 IP 地址分配方案属于逻辑设计文档，设备清单列表属于物理设计文档，集中访谈的信息资料属于需求分析文档，而网络内部通信流量分布属于网络系统分析文档。这 4 种文档分别在逻辑设计阶段、物理设计阶段和网络需求分析阶段产生。

**参考答案**

（69）A　（70）B

**试题（71）～（75）**

Without proper safeguards, every part of a network is vulnerable to a security breach or unauthorized activity from ＿（71）＿, competitors, or even employees. Many of the organizations that manage their own ＿（72）＿ network security and use the Internet for more than just sending/receiving e-mails experience a network ＿（73）＿—and more than half of these companies do not even know they were attacked. Smaller ＿（74）＿ are often complacent, having gained a false sense of security. They usually react to the last virus or the most recent defacing of their website. But they are trapped in a situation where they do not have the necessary time and ＿（75）＿ to spend on security.

（71）A．intruders　B．terminals　C．hosts　D．users

（72）A．exterior　B．internal　C．centre　D．middle
（73）A．attack　B．collapse　C．breakdown　D．virus
（74）A．users　B．campuses　C．companies　D．networks
（75）A．safeguards　B．businesses　C．experiences　D．resources

**参考译文**

如果缺乏适当的安全措施，网络的每一部分对安全部门来说都是脆弱的，特别是遭受来自闯入者、竞争对手甚至内部雇员的未经授权的侵入活动时。很多管理自己内部网络的组织，大部分都使用互联网，而且不仅仅是发送/接收电子邮件，这些公司都经历过网络攻击，大部分甚至还不知道他们被攻击过。那些小公司还会因为虚假的安全感觉而洋洋自得。他们通常只能对最近发现的计算机病毒或者给他们网站造成的损害做出反应。但是他们已经陷入了没有必要的时间和资源来进行安全防护的困境。

**参考答案**

（71）A　（72）B　（73）A　（74）C　（75）D

# 第 30 章　2016 上半年网络工程师下午试题分析与解答

## 试题一（共 20 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业网络拓扑如图 1-1 所示，A～E 是网络设备的编号。

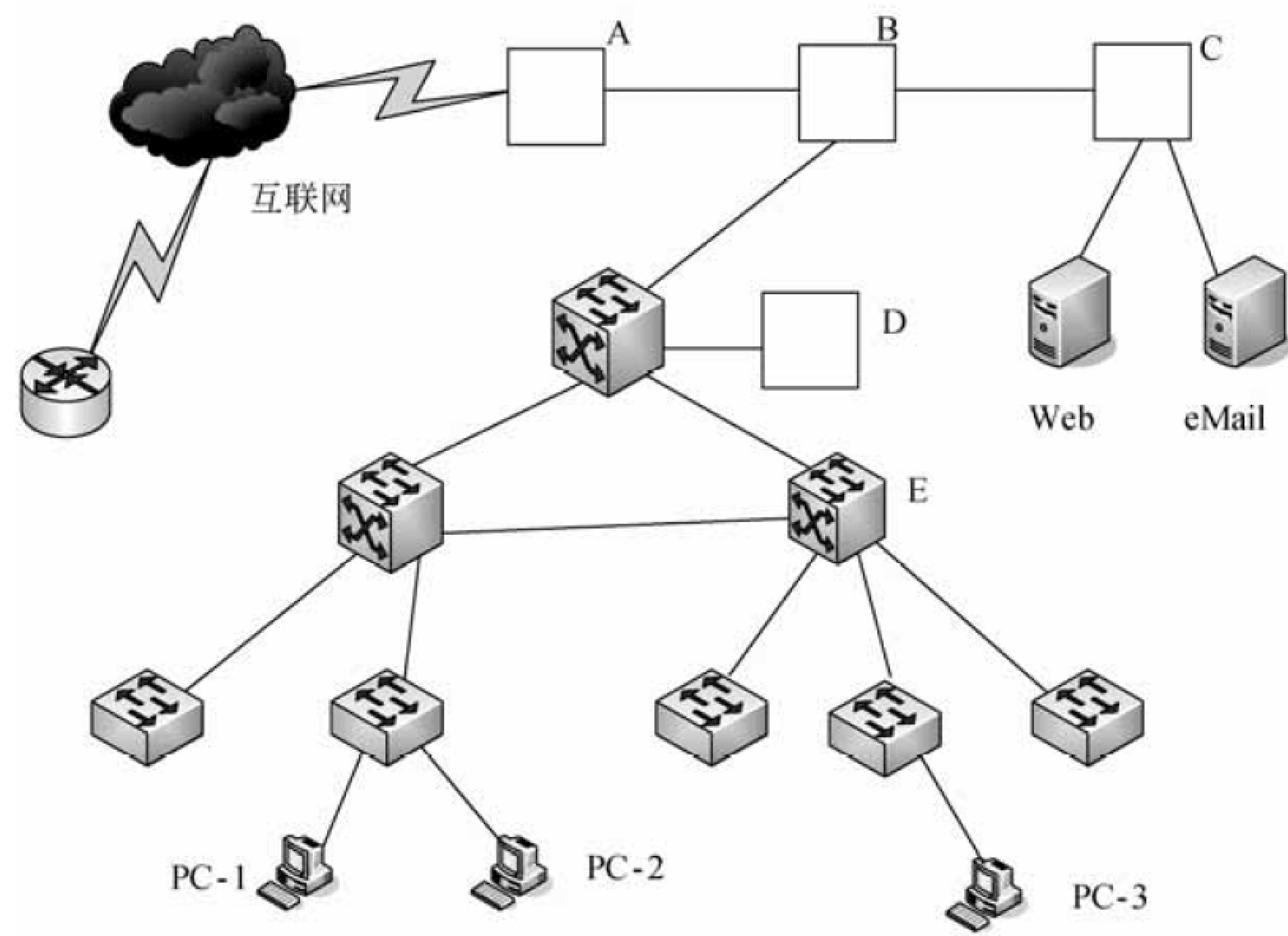



图 1-1

**【问题 1】（每空 1 分，共 4 分）**

根据图 1-1，将设备清单表 1-1 所示内容补充完整。

**表 1-1**

| 设　备　名 | 在图中的编号 |
|---|---|
| 防火墙 USG3000 | （1） |
| 路由器 AR2220 | （2） |
| 交换机 QUIDWAY3300 | （3） |
| 服务器 IBM X3500M5 | （4） |

**【问题 2】（每空 2 分，共 4 分）**

以下是 AR2220 的部分配置。

```
[AR2220]acl 2000
[AR2220-acl-2000]rule normal permit source 192.168.0.0 0.0.255.255
[AR2220-acl-2000]rule normal deny source any
[AR2220-acl-2000]quit
[AR2220]interface Ethernet0
[AR2220-Ethernet0]ip address 192.168.0.1 255.255.255.0
[AR2220-Ethernet0]quit
[AR2220]interface Ethernet1
[AR2220-Ethernet1]ip address 59.41.221.100 255.255.255.0
[AR2220-Ethernet1]nat outbound 2000 interface
[AR2220-Ethernet1]quit
[AR2220]ip route-static 0.0.0.0 0.0.0.0 59.74.221.254
```

设备 AR2220 使用 __（5）__ 接口实现 NAT 功能，该接口地址的网关是 __（6）__。

**【问题 3】（每空 2 分，共 6 分）**

若只允许内网发起 ftp、http 连接，并且拒绝来自站点 2.2.2.11 的 Java Applets 报文。在 USG3000 设备中有如下配置，请补充完整。

```
[USG3000] acl number 3000
[USG3000-acl-adv-3000]rule permit tcp destination-port eq www
[USG3000-acl-adv-3000]rule permit tcp destination-port eq ftp
[USG3000-acl-adv-3000]rule permit tcp destination-port eq ftp-data
[USG3000] acl number 2010
[USG3000-acl-basic-2010] rule __(7)__ source 2.2.2.11 0.0.0.0
[USG3000-acl-basic-2010] rule permit source any
[USG3000]__(8)__ interzone trust untrust
[USG3000-interzone-trust-untrust] packet-filter 3000__(9)__
[USG3000-interzone-trust-untrust] detect ftp
[USG3000-interzone-trust-untrust] detect http
[USG3000-interzone-trust-untrust] detect java-blocking 2010
```

（7）～（9）备选答案：

A．firewall　　B．trust　　C．deny

D．permit　　E．outbound　　F．inbound

**【问题 4】（每空 2 分，共 6 分）**

PC-1、PC-2、PC-3 网络设置如表 1-2。

**表 1-2**

| 设　备　名 | 网 络 地 址 | 网　　关 | VLAN |
| --- | --- | --- | --- |
| PC-1 | 192.168.2.2/24 | 192.168.2.1 | VLAN100 |
| PC-2 | 192.168.3.2/24 | 192.168.3.1 | VLAN200 |
| PC-3 | 192.168.4.2/24 | 192.168.4.1 | VLAN300 |

通过配置 RIP，使得 PC-1、PC-2、PC-3 能相互访问，请补充设备 E 上的配置，或解释相关命令。

```
//配置 E 上 vlan 路由接口地址
interface vlanif 300
ip address __(10)__ 255.255.255.0
interface vlanif 1000              //互通 VLAN
ip address 192.168.100.1  255.255.255.0
//配置 E 上的 rip 协议
rip
network  192.168.4.0
network __(11)__
//配置 E 上的 trunk 链路
int e0/1
port link-type trunk    //__(12)__
      port trunk permit vlan all
```

**试题一分析**

本题考查网络设备配置的相关知识。

此类题目要求考生认真阅读题目中给出的配置文件内容，了解设备需要实现的网络功能。对于路由器、防火墙、交换机等网络设置的部署，应该兼顾不同设备的特点、网络业务和安全需求。

**【问题 1】**

防火墙的防护区域可分为内、外网和 DMZ 区域，在本题网络拓扑中，A 的位置是路由器，在配置文件中定义了外网接口，可以与外部网络进行通信。同时，在路由器上定义 NAT，对内网地址进行了有效屏蔽，也起到了节省公网地址作用。B 的位置是防火墙，可以对内网用户和服务器进行有效保护，抵御来自外部网络的攻击。C 位置是交换机，用于服务器设备的接入。D 的位置是服务器，一般只限于内网访问访问。

**【问题 2】**

设备 AR2220 的配置文件主要定义了内、外网接口，并且配置了内、外网络访问的策略，将内网地址转换成外网接口地址用于访问外部网络。有关命令解释如下。

（1）rule normal permit source 与 rule normal deny source any 命令配合使用，表示源

地址段以外的地址禁止通过。

（2）interface Ethernet0 与 ip address 配合使用，定义设备的接口地址，配置文件中定义了两个接口地址。

（3）nat outbound 2000 interface 命令是在设备上启用了 NAT 规则。

（4）ip route-static 是一条静态路由命令，告诉路由器默认数据的下一跳地址。

【问题 3】

设备 USG3000 的配置文件主要内容是配置内、外网访问策略。有关命令解释如下：

（1）acl number 3000 规则，允许 www、ftp、ftp-data 等协议。

（2）acl number 2010 规则，配置对 HTTP、FTP 协议指定 ASPF 策略。

ASPF（application specific packet filter）是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。包括 dos（denial of service，拒绝服务）的检测和防范。java blocking（java 阻断）保护网络不受有害 java applets 的破坏。activex blocking（activex 阻断）保护网络不受有害 activex 的破坏。

【问题 4】

RIP 协议是动态路由选择协议，通过路由表的自动更新使 IP 进行数据交换时获取正确的路径。

port link-type trunk 定义接口类型，Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口。

## 参考答案

【问题 1】

（1）B

（2）A

（3）C

（4）D

【问题 2】

（5）Ethernet1

（6）59.74.221.254

【问题 3】

（7）C

（8）A

（9）E

【问题 4】

（10）192.168.4.1

（11）192.168.100.0

（12）定义端口为 trunk

**试题二（共 20 分）**

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

**【说明】**

某学校的网络拓扑结构图如图 2-1 所示。

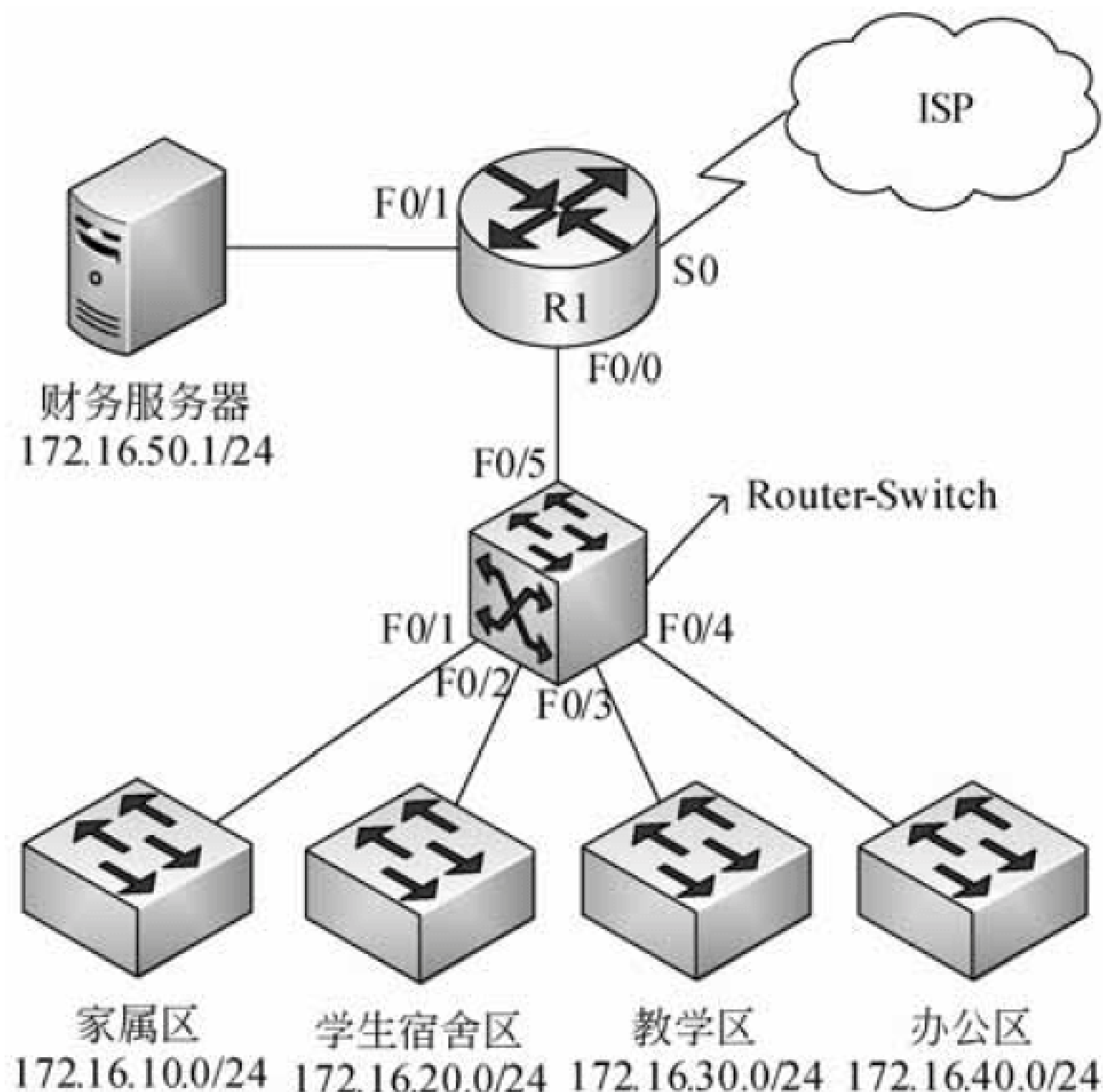



图 2-1

**【问题 1】（每空 1 分，共 7 分）**

常用的 IP 访问控制列表有两种，它们是编号为___（1）___和 1300～1399 的标准访问控制列表和编号为___（2）___和 2000～2699 的扩展访问控制列表。其中，标准访问控制列表是依据 IP 报文的___（3）___来对 IP 报文进行过滤，扩展访问控制列表是依据 IP 报文的___（4）___、___（5）___、上层协议和时间等来对 IP 报文进行过滤。一般地，标准访问控制列表放置在靠近___（6）___的位置，扩展访问控制列表放置在靠近___（7）___的位置。

**【问题 2】（每空 1 分，共 10 分）**

为保障安全，使用 ACL 对网络中的访问进行控制。访问控制的要求如下：

（1）家属区不能访问财务服务器，但可以访问互联网；

（2）学生宿舍区不能访问财务服务器，且在每天晚上 18:00～24:00 禁止访问互联网；

（3）办公区可以访问财务服务器和互联网；

（4）教学区禁止访问财务服务器，且每天 8:00～18:00 禁止访问互联网。

1．使用 ACL 对财务服务器进行访问控制，请将下面配置补充完整。

```
R1(config)#access-list 1 __(8)__ __(9)__ 0.0.0.255
R1(config)#access-list 1 deny 172.16.10.0 0.0.0.255
R1(config)#access-list 1 deny 172.16.20.0 0.0.0.255
R1(config)#access-list 1 deny __(10)__ 0.0.0.255
R1(config)#interface__(11)__
R1(config-if)#ip access-group 1 __(12)__
```

2．使用 ACL 对 Internt 进行访问控制，请将下面配置补充完整。

```
Route-Switch(config)#time-range jxq    //定义教学区时间范围
Route-Switch(config-time-range)#periodic daily __(13)__
Route-Switch(config)#time-range xsssq    //定义学生宿舍区时间范围
Route-Switch(config-time-range)#periodic __(14)__ 18:00 to 24:00
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 100 permit ip 172.16.10.0 0.0.0.255 any
Route-Switch(config)#access-list 100 permit ip 172.16.40.0 0.0.0.255 any
Route-Switch(config)#access-list 100 deny ip __(15)__ 0.0.0.255 time-range jxq
Route-Switch(config)#access-list 100 deny ip __(16)__ 0.0.0.255 time-range
xsssq
Route-Switch(config)#interface __(17)__
Route-Switch(config-if)# ip access-group 100 out
```

**【问题 3】（每空 1 分，共 3 分）**

网络在运行过程中发现，家属区网络经常受到学生宿舍区网络的 DDoS 攻击，现对家属区网络和学生宿舍区网络之间的流量进行过滤，要求家属区网络可访问学生宿舍区网络，但学生宿舍区网络禁止访问家属区网络。

采用自反访问列表实现访问控制，请解释配置代码。

```
Route-Switch(config)#ip access-list extended infilter
Route-Switch(config-ext-nacl)#permit ip any 172.16.20.0 0.0.0.255 reflect
jsq //__(18)__
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#ip access-list extended outfilter
Route-Switch(config-ext-nacl)# evaluate jsq //__(19)__
Route-Switch(config-ext-nacl)#exit
Route-Switch(config)#interface fastethernet 0/1
Route-Switch(config-if)#ip access-group infilter in
Route-Switch(config-if)#ip access-group outfilter out //__(20)__
```

**试题二分析**

本题考查使用访问控制列表实现访问控制的知识。

此类题目要求考生认真研读题目，并对相关基础知识有一定的掌握，并数序访问控制列表的基本配置方法和配置要求。

**【问题 1】**

该问题考查访问控制列表的基础知识及应用，包括 IP 访问控制列表有标准访问控制列表和扩展访问控制列表。

标准访问控制列表有以下特点：

- 编号从 1～99 和 1300～1399；
- 依据 IP 报文的源 IP 地址对数据包进行过滤；
- 部署时应放置于靠近目的网络（或者路由器出口）的位置上。

扩展访问控制列表有以下特点：

- 编号从 100～199 和 2000～2699；
- 依据 IP 报文的源 IP 地址、目的 IP 地址、上层协议、端口号和时间等信息对数据报文进行过滤；
- 部署时应放置于靠近源地址（或者路由器入口）的位置上。

**【问题 2】**

根据题干给出网络安全需求，访问控制列表的配置方法，以及给出的部分配置代码，是使用标准访问控制列表 access-list 1 对财务服务器的访问进行控制。允许办公区（172.16.40.0）网段访问，并将 access-list 1 应用在靠近目的端的 R1 的 fastethernet 0/1 接口的出口方向。

创建扩展访问控制列表 access-list 100 来实现用户对于 Internet 的访问，并创建与题目要求相应的时间段，分别设置允许和拒绝的网段，并应用相应的时间段，将应用在 Route-Switch 设备的 F0/5 接口的出方向。

**【问题 3】**

该问题要求考生理解自反访问控制列表的工作机制和配置方法。根据题干描述，家属区网络收到学生宿舍网络发出的 DdoS 攻击报文，为了避免该现象，要求家属区网络可以访问学生宿舍网络，反之不可。该应用场景是自反访问控制列表的典型应用场景。根据一个方向的访问控制列表，自动创建出一个反方向的控制列表，是和原来的控制列表—IP 的源地址和目的地址颠倒，并且源端口号和目的端口号完全相反的一个列表。

**参考答案**

**【问题 1】**

（1）1～99

（2）100～199

（3）源 IP 地址

（4）源 IP 地址

（5）目标 IP 地址

（6）目标地址（或出口）

（7）源地址（或入口）

注：（4）、（5）答案可互换

**【问题 2】**

（8）permit

（9）172.16.40.0

（10）172.16.30.0

（11）fastethernet 0/1（或 f0/1）

（12）out

（13）8:00 to 18:00

（14）daily

（15）172.16.30.0

（16）172.16.20.0

（17）f0/5

**【问题 3】**

（18）建立 jsq 的 ACL 映射表

（19）允许 jsq 映射表的连接通过

（20）应用 outfilter 规则到 fastethernet 0/1 接口的出方向

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业采用 Windows Server 2003 配置了 DHCP、DNS 和 Web 服务。

**【问题 1】（每空 1 分，共 4 分）**

DHCP 服务器地址池 192.168.0.1～192.168.0.130，其中 192.168.0.10 分配给网关，192.168.0.11～192.168.0.15 分配给服务器，192.168.0.20 分配给网络管理员。

图 3-1

图 3-2

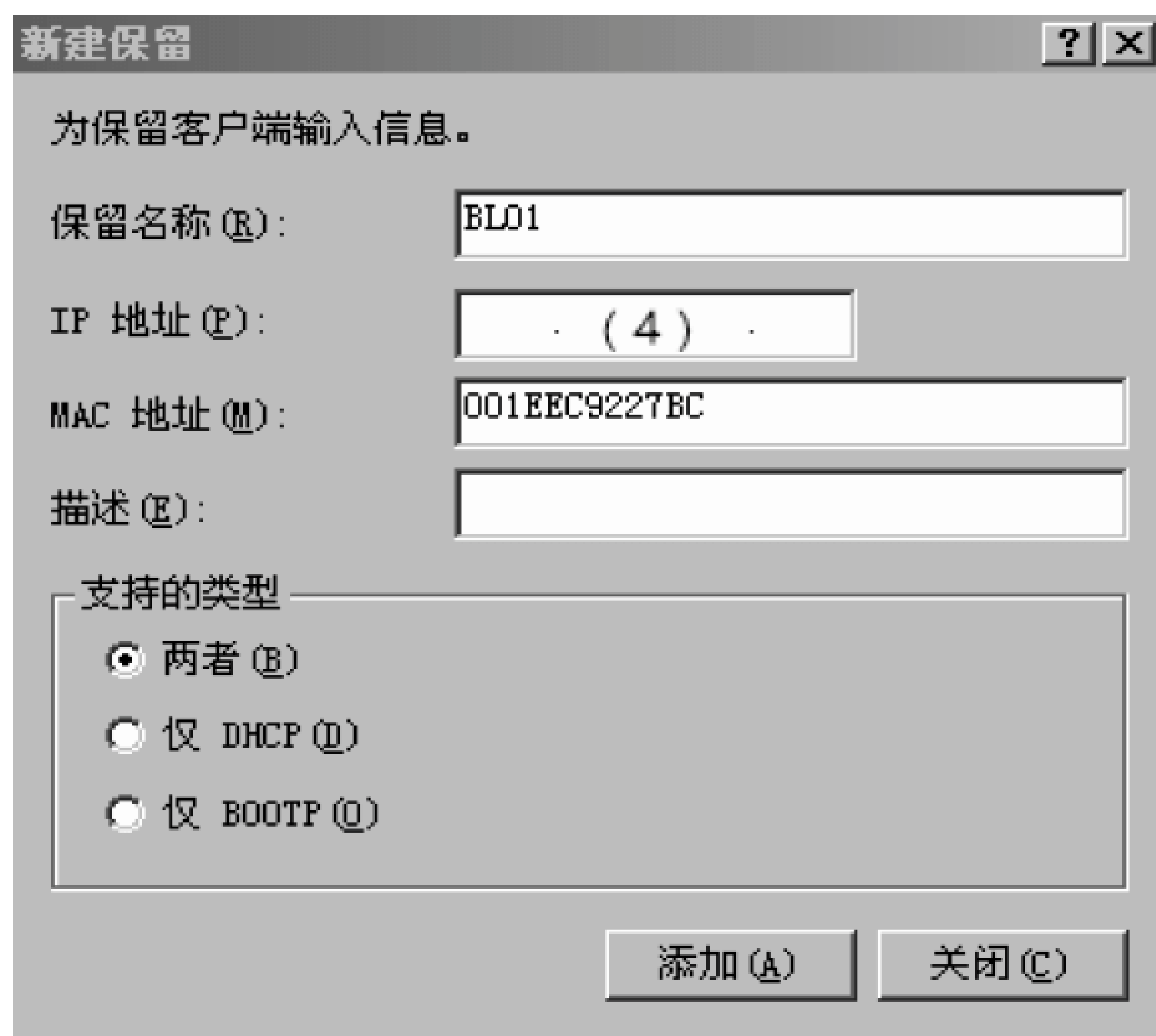



图 3-3

请填充图 3-1 至图 3-3 中（1）～（4）处空缺内容。

**【问题 2】（每空 1.5 分，共 9 分）**

DNS 的配置如图 3-4 所示。

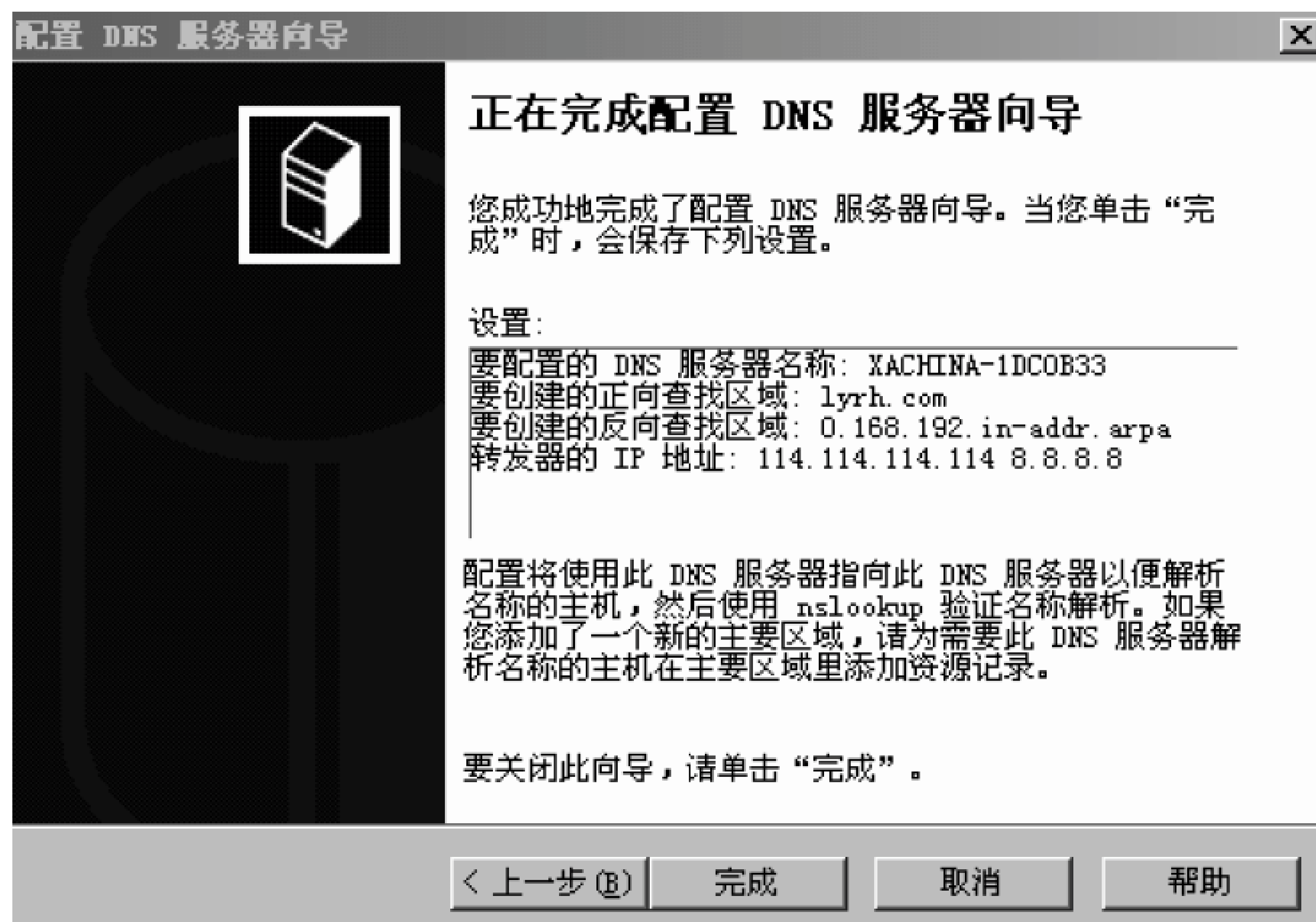



图 3-4

根据图 3-4 判断正误（正确的答“对”，错误的答“错”）。

A．XACHINA-1DC0B33 的 IP 地址为 114.114.114.114。 （5）

B．该域名服务器无法解析的域名转发到 114.114.114.114 或 8.8.8.8。（6）

C．域 lyrh.com 的资源记录包含在该 DNS 服务器中。 （7）

D．客户机的“首选 DNS 服务器”地址必须与该 DNS 服务器地址一致。（8）

E．该域名服务器是 lyrh.com 的授权域名服务器。（9）。

F．该域名服务器支持 192.168.101.6 地址的反向域名查找。（10）。

**【问题 3】（每空 2 分，共 4 分）**

Web 服务器的配置如图 3-5 所示。




图 3-5

1. 如图 3-5 所示，通过主机头的方式建立两个网站 www.ycch.com 和 www.lyrh.com，网站配置是＿（11）＿。

（11）备选答案：

A．相同的 IP 地址，不同的端口号

B．不同的 IP 地址，相同的目录

C．相同的 IP 地址，不同的目录

D．相同的主机头，相同的端口号

2．除了主机头方式，还可以采用＿（12）＿方式在一台服务器上配置多网站。

**【问题 4】（每空 1 分，共 3 分）**

Windows Server 2003 管理界面如图 3-6 所示。

1．图 3-6 中设备打“？”的含义是＿（13）＿；设备打“×”的含义是＿（14）＿。

2．图 3-6 中 1394 网络适配器能连接什么设备？＿（15）＿。




图 3-6

**试题三分析**

本题考查 Windows Server 2003 配置 DHCP、DNS 和 Web 服务的知识。此类题目要求考生熟悉相关网络服务的配置界面以及参数设置的含义。

**【问题 1】**

IP 地址范围指地址池中所有地址，用起始地址和结束地址表示整个地址池。排除地址指的是 DHCP 服务器对在地址池中不用于动态分配的地址，该地址在任何时候都不会被 DHCP 服务器分配给客户机，排除地址常用于需要固定分配 IP 的网关、服务器等。保留地址是指 DHCP 服务器会将该地址始终分配给特定客户端。

**【问题 2】**

114.114.114.114 与 8.8.8.8 是互联网中主要的 DNS 服务器，本地域名服务器无法解析时可以转发到此类服务器上。

每个区域数据库文件都是由资源记录构成的，主要有 SOA 记录、NS 记录、A 记录、CNAME 记录、MX 记录和 PTR 记录等。本地域的资源记录应当包含在本地的 DNS 服务器中。

客户机的“首选 DNS 服务器”地址一般选取性能稳定，解析速度快的 DNS 服务器。

地址 192.168.101.6 不包含在 DNS 的反向搜索区域中，因此不支持对该地址的反向域名查找。

**【问题 3】**

通常情况下一个IP 地址和80 端口只能正确对应一个网站，处理一个域名的访问请

求。而 Web 服务器在不使用多个 IP 地址和端口的情况下，如果要支持多个相对独立的网站，就需要采用一种机制来分辨同一个 IP 地址上的不同网站的请求，即主机头绑定的方法。将不同的网站空间对应不同的域名，通过域名字段来分发和应答对应空间的文件执行结果。

除了主机头绑定的方式以外，可以在一个网卡上绑定多个 IP 地址，或者是采用相同 IP 地址配合不同端口号实现多个域名的访问。

**【问题 4】**

Windows 操作系统采用图形化界面，在设备管理中，设备采用简洁、容易识别的图标显示，设备只有在安装正确的驱动程序后才能被系统所使用。当设备驱动未安装或者设备禁止使用时，在设备管理界面相应位置会以特定图标显示，提醒用户系统存在设备配置问题。

IEEE 1394 是一种串行数据传输协议，支持在运行的计算机上拔插设备。相对于同样是串行总线的 USB，传输带宽更高，可用于数码照相机或便携音频播放器，外接硬盘等高带宽应用。

**参考答案**

**【问题 1】**

（1）192.168.0.1

（2）192.168.0.130

（3）192.168.0.10 到 102.168.0.15

（4）192.168.0.20

**【问题 2】**

（5）错

（6）对

（7）对

（8）错

（9）对

（10）错

**【问题 3】**

（11）C

（12）网卡绑定多个 IP 地址

或 同一 IP 地址+不同的端口号（任选一个）

**【问题 4】**

（13）未安装驱动

（14）禁用

（15）数码设备，大容量硬盘，1394 扫描仪等。（任选一个）

## 试题四（共 15 分）

阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。

【说明】

某公司有 3 个分支机构，网络拓扑结构及地址分配如图 4-1 所示。

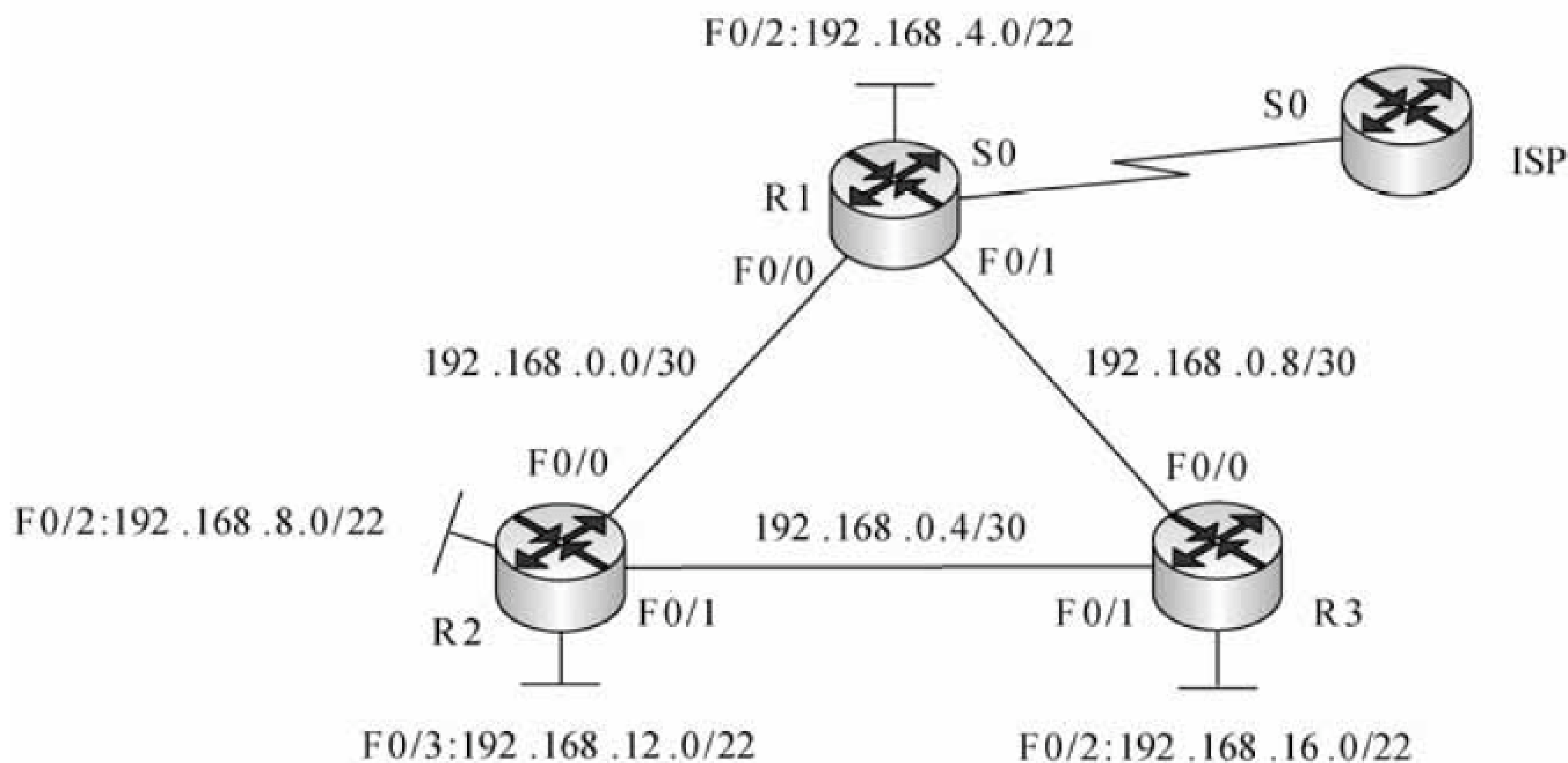



图 4-1

【问题 1】（每空 1 分，共 11 分）

公司申请到 202.111.1.0/29 的公有地址段，采用 NAPT 技术实现公司内部访问互联网的要求，其中，192.168.16.0/22 网段禁止访问互联网。R1、R2 和 R3 的基本配置已正确配置完成，其中 R1 的配置如下。请根据拓扑结构，完成下列配置代码。

R1 的基本配置及 NAPT 配置如下：

```
R1>enable
R1#config terminal
R1(config)#interface fastenthernet 0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastenthernet 0/1
R1(config-if)#ip address 192.168.0.9 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastenthernet 0/2
R1(config-if)#ip address ___(1)___ 255.255.252.0    //使用网段中最后一个地址
R1(config-if)#no shutdown
```

```
R1(config-if)#exit
R1(config)#interface serial 0
R1(config-if)#ip address 202.111.1.1 255.255.255.248
R1(config-if)#no shutdown
R1(config)#ip nat pool ss 202.111.1.1 ___(2)___ netmask ___(3)___
R1(config)# interface___(4)___ fastenthernet 0/0-1
R1(config-if)#ip nat ___(5)___
R1(config-if)#interface serial 0
R1(config-if)#ip nat ___(6)___
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.0.0 ___(7)___
R1(config)#ip nat inside ___(8)___ list ___(9)___ pool ___(10)___ ___(11)___
```

**【问题 2】（每空 2 分，共 4 分）**

在 R1、R2 和 R3 之间运行 OSPF 路由协议，其中 R1、R2 和 R3 的配置如下。

```
行号    配置代码
1       R1(config)#router ospf 1
2       R1(config-router)#network 192.168.4.0 0.0.3.255 area 0
3       R1(config-router)#network 192.168.0.0 0.0.0.3 area 0
4       R1(config-router)#network 192.168.0.8 0.0.0.3 area 0

5       R2>enable
6       R2#config terminal
7       R2(config)#router ospf 2
8       R2(config-router)#network 192.168.8.0 0.0.3.255 area 0
9       R2 (config-router)#network 192.168.12.0 0.0.3.255 area 0
10      R2 (config-router)#network 192.168.0.4 0.0.0.3 area 0

11      R3>enable
12      R3#config terminal
13      R3(config)#router ospf 3
14      R3(config-router)#network 192.168.0.8 0.0.0.3 area 0
15      R3(config-router)#network 192.168.0.4 0.0.0.3 area 0
```

1. 配置完成后，在 R1 和 R2 上均无法 ping 通 R3 的局域网，可能的原因是___（12）___。

（12）备选答案：

A．在 R3 上未宣告局域网路由　　B．以上配置中第 7 行和第 13 行配置错误

C．第 1 行配置错误　　D．R1、R2 未宣告直连路由

2．在 OSPF 中重分布默认路由的命令是：（13）。

（13）备选答案：

A．R1#default-information originate

B．R1(config-if)#default-information originate

C．R1(config-router)#default-information originate

D．R1(config)#default-information originate

**试题四分析**

本题考查交换机路由器的基本配置 NAT 的配置方法方面的知识。

此类题目要求考生认真阅读题目要求，细致观察图中所示的拓扑结构和 IP 地址，并熟练掌握交换机路由器的配置方法和配置命令。

**【问题 1】**

在路由器 R1 上创建相应的 NAPT 地址池并将内部地址进行转换，由于使用的是动态地址转换，因此需要使用关键字 overload。

**【问题 2】**

根据题目给出的相关配置可知，R1 和 R2 均无法 ping 通 R3 的局域网，表明在 R1 和 R2 上不存在 R3 局域网的路由条目，最可能的原因是在 R3 上未宣告其局域网路由。

在 OSPF 路由协议中，重分布默认路由的命令是在路由协议配置模式先使用 default-information originate 命令。

**参考答案**

**【问题 1】**

（1）192.168.7.254

（2）202.111.1.5

（3）255.255.255.248

（4）range

（5）inside

（6）outside

（7）0.0.15.255

（8）source

（9）1

（10）ss

（11）overload

**【问题 2】**

（12）A

（13）C

# 第 31 章　2016 下半年网络工程师上午试题分析与解答

**试题（1）**

在程序运行过程中，CPU 需要将指令从内存中取出并加以分析和执行。CPU 依据__（1）__来区分在内存中以二进制编码形式存放的指令和数据。

（1）A．指令周期的不同阶段　　B．指令和数据的寻址方式
　　C．指令操作码的译码结果　　D．指令和数据所在的存储单元

**试题（1）分析**

本题考查计算机系统基础知识。

指令周期是执行一条指令所需要的时间，一般由若干个机器周期组成，是从取指令、分析指令到执行完所需的全部时间。CPU 执行指令的过程中，根据时序部件发出的时钟信号按部就班进行操作。在取指令阶段读取到的是指令，在分析指令和执行指令时，需要操作数时再去读操作数。

**参考答案**

（1）A

**试题（2）分析**

计算机在一个指令周期的过程中，为从内存读取指令操作码，首先要将__（2）__的内容送到地址总线上。

（2）A．指令寄存器（IR）　　B．通用寄存器（GR）
　　C．程序计数器（PC）　　D．状态寄存器（PSW）

**试题（2）分析**

本题考查计算机系统基础知识。

CPU 首先从程序计数器（PC）获得需要执行的指令地址，从内存（或高速缓存）读取到的指令则暂存在指令寄存器（IR），然后进行分析和执行。

**参考答案**

（2）C

**试题（3）**

设 16 位浮点数，其中阶符 1 位、阶码值 6 位、数符 1 位、尾数 8 位。若阶码用移码表示，尾数用补码表示，则该浮点数所能表示的数值范围是__（3）__。

（3）A．$-2^{64} \sim (1-2^{-8})2^{64}$　　B．$-2^{63} \sim (1-2^{-8})2^{63}$
　　C．$-(1-2^{-8})2^{64} \sim (1-2^{-8})2^{64}$　　D．$-(1-2^{-8})2^{63} \sim (1-2^{-8})2^{63}$

**试题（3）分析**

本题考查计算机系统基础知识。

浮点格式表示一个二进制数 N 的形式为 $N=2^E\times F$，其中 E 称为阶码，F 叫作尾数。在浮点表示法中，阶码通常为含符号的纯整数，尾数为含符号的纯小数。

指数为纯整数，阶符 1 位、阶码 6 位在补码表示方式下可表示的最大数为 63($2^6-1$)，最小数为−64($-2^6$)。尾数用补码表示时最小数为−1、最大数为$1-2^{-8}$，因此该浮点表示的最小数为$-2^{63}$，最大数为$(1-2^{-8})\times 2^{63}$。

**参考答案**

（3）B

**试题（4）**

已知数据信息为 16 位，最少应附加__（4）__位校验位，以实现海明码纠错。

（4）A．3　　B．4　　C．5　　D．6

**试题（4）分析**

本题考查计算机系统基础知识。

海明码是利用奇偶性来检错和纠错的校验方法。海明码的构成方法是：在数据位之间插入 $k$ 个校验位，通过扩大码距来实现检错和纠错。

设数据位是 $n$ 位，校验位是 $k$ 位，则 $n$ 和 $k$ 必须满足以下关系：$2^k-1\geqslant n+k$

若数据信息为 $n$=16 位，则 $k$=5 是满足 $2^k-1\geqslant n+k$ 的最小值。

**参考答案**

（4）C

**试题（5）**

将一条指令的执行过程分解为取指、分析和执行三步，按照流水方式执行，若取指时间 $t_{取指}=4\Delta t$、分析时间 $t_{分析}=2\Delta t$、执行时间 $t_{执行}=3\Delta t$，则执行完 100 条指令，需要的时间为__（5）__$\Delta t$。

（5）A．200　　B．300　　C．400　　D．405

**试题（5）分析**

本题考查计算机系统基础知识。

对于该指令流水线，建立时间为 $4\Delta t+2\Delta t+3\Delta t=9\Delta t$，此后每 $4\Delta t$ 执行完一条指令，即执行完 100 条指令的时间为 $9\Delta t+99*4\Delta t=405\Delta t$。

**参考答案**

（5）D

**试题（6）**

在敏捷过程的开发方法中，__（6）__使用了迭代的方法，其中，把每段时间（30 天）一次的迭代称为一个“冲刺”，并按需求的优先级别来实现产品，多个自组织和自治的小组并行地递增实现产品。

（6）A．极限编程 XP　　B．水晶法
　　C．并列争球法　　D．自适应软件开发

**试题（6）分析**

本题考查敏捷方法的基础知识。

在 20 世纪 90 年代后期，一些开发人员抵制严格化软件开发过程，试图强调灵活性在快速有效的软件生产中的作用，提出了敏捷宣言，即个人和交互胜过过程和工具；可以运行的软件胜过面面俱到的文档；与客户合作胜过合同谈判；对变化的反应胜过遵循计划。

基于这些基本思想，有很多敏捷过程的典型方法。其中，极限编程 XP 是激发开发人员创造性、使得管理负担最小的一组技术；水晶法 Crystal 认为每一个不同的项目都需要一套不同的策略、约定和方法论；并列争球法（Scrum）使用迭代的方法，其中把每 30 天一次的迭代成为一个冲刺，并按需求的优先级来实现产品。多个自组织和自治小组并行地递增实现产品，并通过简短的日常情况会议进行协调。

自适应软件开发（ASD）有六个基本的原则：

① 在自适应软件开发中，有一个使命作为指导，它设立了项目的目标，但并不描述如何达到这个目标；

② 特征被视为客户键值的关键，因此，项目是围绕着构造的构件来组织并实现特征；

③ 过程中的迭代是很重要的，因此重做与做同样重要，变化也包含其中；

④ 变化不视为是一种更正，而是对软件开发实际情况的调整；

⑤ 确定的交付时间迫使开发人员认证考虑每一个生产版本的关键需求；

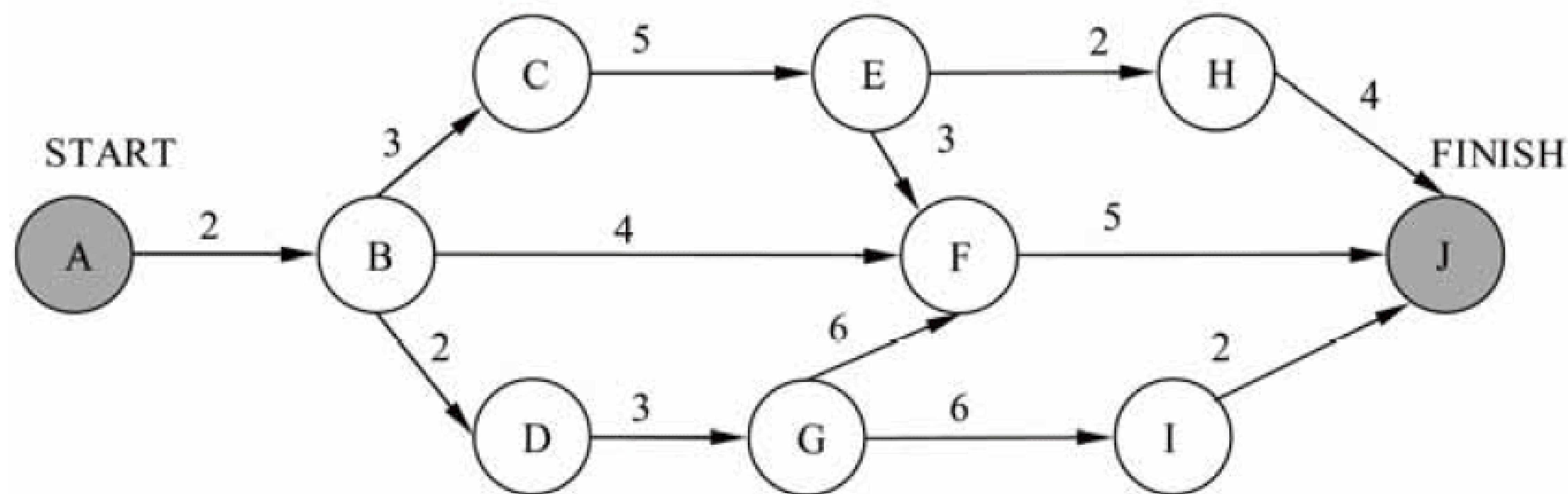
⑥ 风险也包含其中，它使开发人员首先跟踪最艰难的问题。

**参考答案**

（6）C

**试题（7）、（8）**

某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示相应活动的持续时间（天），则完成该项目的最少时间为＿（7）＿天。活动 BC 和 BF 最多可以晚开始＿（8）＿天而不会影响整个项目的进度。



（7）A. 11　　B. 15　　C. 16　　D. 18

（8）A. 0 和 7　　B. 0 和 11　　C. 2 和 7　　D. 2 和 11

**试题（7）、（8）分析**

本题考查软件项目管理的基础知识。

活动图是描述一个项目中各个工作任务相互依赖关系的一种模型，项目的很多重要特性可以通过分析活动图得到，如估算项目完成时间，计算关键路径和关键活动等。

根据上图计算出关键路径为 A→B→C→E→F→J 和 A→B→D→G→F→J，其长度为 18。关键路径上的活动均为关键活动。活动 BC 在关键路径上，因此松弛时间为 0。活动 BF 不在关键路径上，包含该活动的最长路径为 A→B→F→J，其长度为 11，因此该活动的松弛时间为 18−11=7。

**参考答案**

（7）D　（8）A

**试题（9）**

假设系统有 n 个进程共享资源 R，且资源 R 的可用数为 3，其中 n≥3。若采用 PV 操作，则信号量 S 的取值范围应为__（9）__。

（9）A. −1～n−1　　B. −3～3　　C. −(n−3)～3　　D. −(n−1)～1

**试题（9）分析**

本题考查操作系统进程管理中信号量与同步互斥方面的基本知识。

本题中已知有 n 个进程共享 R 资源，且 R 资源的可用数为 3，故信号量 S 的初值应设为 3。当第 1 个进程申请资源时，信号量 S 减 1，即 S=2；当第 2 个进程申请资源时，信号量 S 减 1，即 S=1；当第 3 个进程申请资源时，信号量 S 减 1，即 S=0；当第 4 个进程申请资源时，信号量 S 减 1，即 S=−1；……；当第 n 个进程申请资源时，信号量 S 减 1，即 S=−(n−3)。

**参考答案**

（9）C

**试题（10）**

甲、乙两厂生产的产品类似，且产品都拟使用“B”商标。两厂于同一天向商标局申请商标注册，且申请注册前两厂均未使用“B”商标。此情形下，__（10）__能核准注册。

（10）A. 甲厂　　B. 由甲、乙厂抽签确定的厂

C. 乙厂　　D. 甲、乙两厂

**试题（10）分析**

我国商标注册以申请在先为原则，使用在先为补充。当两个或两个以上申请人在同一种或者类似商品上申请注册相同或者近似商标时，申请在先的人可以获得注册。对于同日申请的情况，商标法及其实施条例规定保护先用人的利益，使用在先的人可以获得

注册“使用”包括将商标用于商品、商品包装、容器以及商品交易书上，或者将商标用于广告宣传、展览及其他商业活动中。如果同日使用或均未使用，则采取申请人之间协商解决，不愿协商或者协商不成的，由各申请人抽签决定。商标局通知各申请人以抽签的方式确定一个申请人，驳回其他人的注册申请。商标局已经通知但申请人未参加抽签的，视为放弃申请。

**参考答案**

（10）B

**试题（11）**

能隔离局域网中广播风暴、提高带宽利用率的设备是＿（11）＿。

（11）A．网桥　　B．集线器　　C．路由器　　D．交换机

**试题（11）分析**

可以根据网络互连设备工作的协议层对其进行分类。中继器（Repeater）工作于物理层，只是起到扩展传输距离的作用，对高层协议是透明的。集线器的工作原理基本上与中继器相同。简单地说，集线器就是一个多端口中继器，它把一个端口上收到的数据广播到所有其他端口上。

网桥（Bridge）工作于数据链路层，网桥检查帧的源地址和目标地址，如果目标地址和源地址不在同一个网段上，就把帧转发到另一个网段上。以太网中广泛使用的交换机（Switch）是一种多端口网桥，每一个端口都可以连接一个局域网。由网桥或交换机连接的各个子网组成一个更大的局域网，形成一个广播域。

路由器（Router）工作于网络层。路由器根据网络层地址（通常是 IP 地址）在互连的子网之间传递分组。路由器连接的各个子网属于不同的局域网，路由器隔离了各个局域网的广播帧，从而抑制了网络中的广播风暴，提高了网络带宽利用率。

网关（Gateway）用于连接网络层之上执行不同协议的子网，组成异构型的互连网络。网关能对互不兼容的高层协议进行转换。

**参考答案**

（11）C

**试题（12）**

点对点协议 PPP 中 LCP 的作用是＿（12）＿。

（12）A．包装各种上层协议　　B．封装承载的网络层协议
　　C．把分组转变成信元　　D．建立和配置数据链路

**试题（12）分析**

PPP 是一组协议，其中包括：

- 链路控制协议 LCP（Link Control Protocol），用于建立、释放和测试数据链路，以及协商数据链路参数；
- 网络控制协议 NCP（Network Control Protocol）用于协商网络层参数，例如动态

分配 IP 地址等；

- 身份认证协议，用于通信双方确认对方的链路标识。

**参考答案**

（12）D

**试题（13）**

TCP/IP 网络中的__（13）__实现应答、排序和流控功能。

（13）A．数据链路层　B．网络层　C．传输层　D．应用层

**试题（13）分析**

TCP/IP 网络中实现应答、排序和流控功能的是传输层协议 TCP。TCP 实现面向连接的传输服务，利用可变大小的滑动窗口协议实现流量控制和应答，并在传输实体缓冲区中进行排序和重传纠错。

**参考答案**

（13）C

**试题（14）、（15）**

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 1 位终止位，每秒钟传送 100 个字符，采用 DPSK 调制，则码元速率为__（14）__，有效数据速率为__（15）__。

（14）A．200 波特　B．500 波特　C．1000 波特　D．2000 波特

（15）A．200b/s　B．500b/s　C．700b/s　D．1000b/s

**试题（14）、（15）分析**

这种通信系统中，每个字符需要 10 位，每秒传送 100 个字符，所以码元速率为 100×10=1000 波特。在每秒传送的 1000 比特中只有 7 位数据位，所以有效数据速率是 700b/s。

**参考答案**

（14）C　（15）C

**试题（16）、（17）**

E1 载波的数据速率是__（16）__Mb/s，E3 载波的数据速率是__（17）__Mb/s。

（16）A．1.544　B．2.048　C．8.448　D．34.368

（17）A．1.544　B．2.048　C．8.448　D．34.368

**试题（16）、（17）分析**

ITU-T 的 E1 信道的数据速率是 2.048 Mb/s。这种载波把 32 个 8 位一组的数据样本组装成 125μs 的基本帧，其中 30 个子信道用于话音传送数据，2 个子信道（CH0 和 CH16）用于传送控制信令。

按照 ITU-T 的多路复用标准，E2 载波由 4 个 E1 载波组成，数据速率为 8.448Mb/s。E3 载波由 4 个 E2 载波组成，数据速率为 34.368 Mb/s。

**参考答案**

（16）B　（17）D

**试题（18）**

IPv6 的链路本地地址是在地址前缀 1111 1110 10 之后附加＿（18）＿形成的。

（18）A．IPv4 地址　　B．MAC 地址

C．主机名　　D．随机产生的字符串

**试题（18）分析**

IPv6 的链路本地地址是在前缀 1111 1110 10 之后附加 MAC 地址形成的，用于同一链路的相邻结点间通信。链路本地地址相当于 IPv4 中的自动专用 IP 地址（APIPA），可用于邻居发现，并且总是自动配置的。

**参考答案**

（18）B

**试题（19）**

连接终端和数字专线的设备 CSU/DSU 被集成在路由器的＿（19）＿端口中。

（19）A．RJ-45 端口　　B．同步串口

C．AUI 端口　　D．异步串口

**试题（19）分析**

CSU/DSU 是用于连接终端和数字专线的设备，它属于 DCE。通常 CSU/DSU 被整合成单一的硬件设备，集成在路由器的同步串口上。

通道服务单元 CSU（Channel Service Unit）是把终端用户和本地数字电话环路相连的数字接口设备。CSU 接收和传送来往于 WAN 线路的信号，并提供对两边线路干扰的屏蔽功能。CSU 也可以响应电话公司用于检测目标的回响信号。

数据服务单元 DSU（Data Service Unit）能够把 DTE 设备上的物理层接口适配到 T1 或者 E1 等通信设施上。DSU 能进行线路控制，把输入的 RS-232C、RS-449或局域网的 V.35 帧转换成 T-1 线路上的 TDM DSX 帧。DSU 也管理分时错误和信号再生，以及信号计时等功能。

CSU/DSU 有时作为独立的产品，有时和路由器集成。

**参考答案**

（19）B

**试题（20）**

下面哪个协议可通过主机的逻辑地址查找对应的物理地址？＿（20）＿

（20）A．DHCP　　B．SMTP　　C．SNMP　　D．ARP

**试题（20）分析**

在 Internet 中用地址分解协议（Address Resolution Protocol。ARP）来实现逻辑地址到物理地址的映像。ARP 分组的格式如下图所示，各字段的含义解释如下：

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td>操作类型</td></tr>
<tr><td colspan="3">发送结点硬件地址</td></tr>
<tr><td colspan="3">发送结点协议地址</td></tr>
<tr><td colspan="3">目标结点硬件地址</td></tr>
<tr><td colspan="3">目标结点协议地址</td></tr>
</table>

- 硬件类型：网络接口硬件的类型，对以太网此值为 1。
- 协议类型：发送方使用的协议，0800H 表示 IP 协议。
- 硬件地址长度：对以太网，地址长度为 6 字节。
- 协议地址长度：对 IP 协议，地址长度为 4 字节。
- 操作类型：
  - ■ 1——ARP 请求
  - ■ 2——ARP 响应
  - ■ 3——RARP 请求
  - ■ 4——RARP 响应

通常 Internet 应用程序把要发送的报文交给 IP 协议，IP 实体当然知道接收方的逻辑地址（否则就不能通信了），但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路实体之前可以用两种方法得到目标物理地址：

（1）查找本地内存中的 ARP 表，这是 IP 地址和以太网地址的映像表。

（2）如果在 ARP 表里查不到，就广播一个 ARP 请求分组，这种分组经过路由器进一步转发，可以到达所有连网的主机。它的含义是："如果你的 IP 地址是这个分组中的目标地址，请回答你的物理地址是什么"。收到该分组的主机一方面可以用分组中的源地址更新自己的 ARP 地址映像表，另一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址，若不相符则不予回答。

**参考答案**

（20）D

**试题（21）**

下面的应用层协议中通过 UDP 传送的是__（21）__。

（21）A. SMTP　　B. TFTP　　C. POP3　　D. HTTP

**试题（21）分析**

应用层协议 SMTP、POP3 和 HTTP 都是通过 TCP 传送，TCP 提供面向连接的传输服务。而 TFTP 是通过 UDP 传送，UDP 提供无连接的传输服务。

**参考答案**

（21）B

**试题（22）**

代理 ARP 是指＿（22）＿。

（22）A．由邻居交换机把 ARP 请求传送给远端目标
　　B．由一个路由器代替远端目标回答 ARP 请求
　　C．由 DNS 服务器代替远端目标回答 ARP 请求
　　D．由 DHCP 服务器分配一个回答 ARP 请求的路由器

**试题（22）分析**

代理 ARP 是指由路由器代替远端目标回答 ARP 请求。当目标端和源端不是通过交换机直接相连，而是被路由器隔离成不同的子网时，就由路由器代表目标端回答源端发送的 ARP 请求，源端就把路由器的 MAC 地址当成目标端的 MAC 地址，所以此后源端和目标端之间的通信都是通过路由器进行转发的。

**参考答案**

（22）B

**试题（23）**

如果路由器收到了多个路由协议转发的、关于某个目标的多条路由，它如何决定采用哪个路由？＿（23）＿

（23）A．选择与自己路由协议相同的　　B．选择路由费用最小的
　　C．比较各个路由的管理距离　　D．比较各个路由协议的版本

**试题（23）分析**

各种路由来源的管理距离如下表所示。

| 路 由 来 源 | 管 理 距 离 | 路 由 来 源 | 管 理 距 离 |
|---|---|---|---|
| 直连路由 | 0 | IS-IS | 115 |
| 静态路由 | 1 | RIP | 120 |
| EIGRP 汇总路由 | 5 | EGP | 140 |
| 外部 BGP | 20 | ODR（按需路由） | 160 |
| 内部 EIGRP | 90 | 外部 EIGRP | 170 |
| IGRP | 100 | 内部 BGP | 200 |
| OSPF | 110 | 未知 | 255 |

如果路由器收到了由多个路由协议转发的、关于某个目标的多条路由，则比较各个路由的管理距离，并采用管理距离小的路由来源提供的路由信息。

**参考答案**

（23）C

**试题（24）**

下面的选项中属于链路状态路由选择协议的是 （24） 。

（24）A．OSPF　　B．IGRP　　C．BGP　　D．RIPv2

**试题（24）分析**

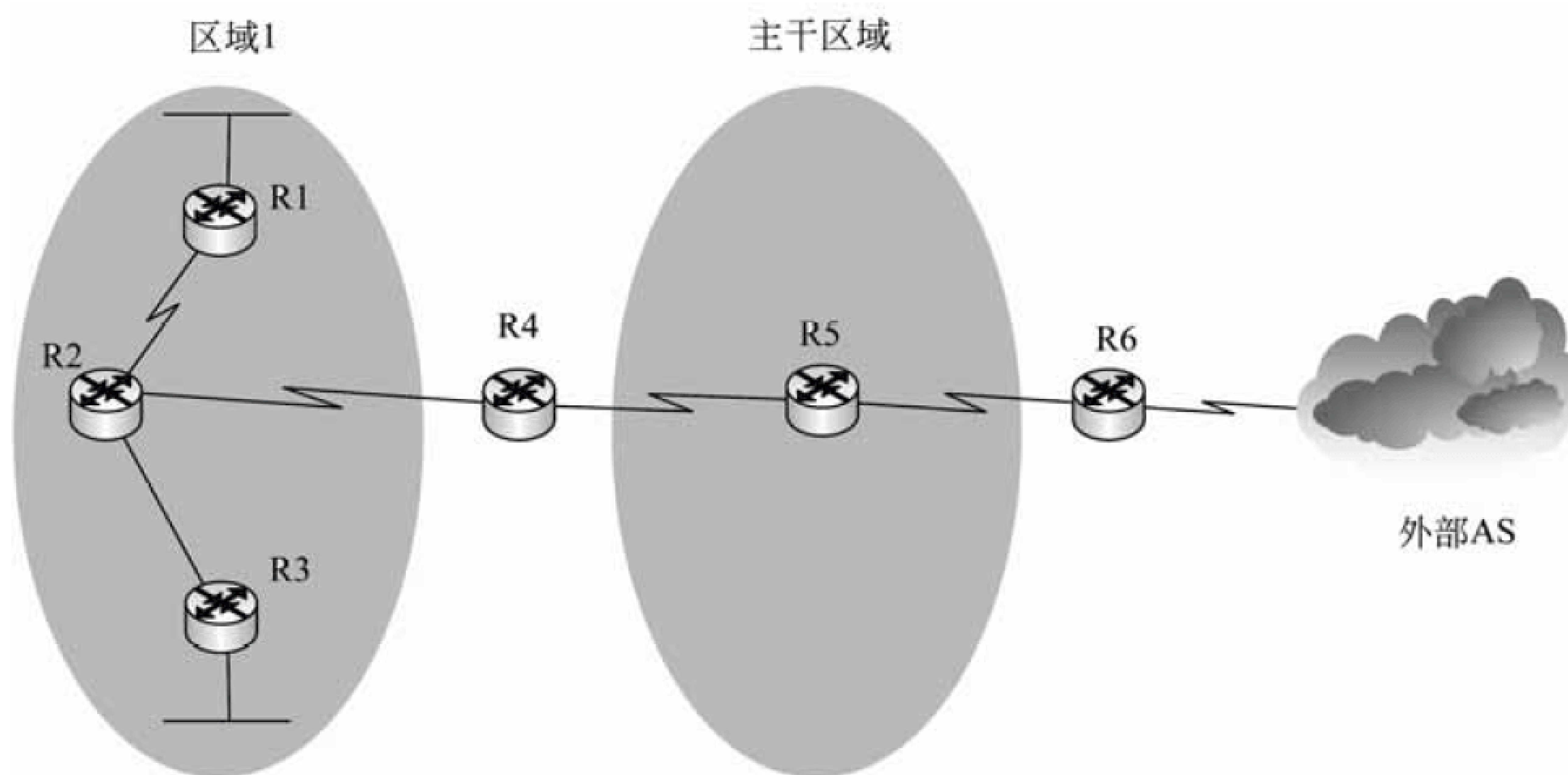
本题选项中属于链路状态路由协议的是 OSPF，RIP 和 IGRP 都是距离矢量路由协议，BGP 是为了控制路由策略的，并不是纯粹计算最短通路的协议。

**参考答案**

（24）A

**试题（25）、（26）**

下面的 OSPF 网络由多个区域组成。在这些路由器中，属于主干路由器的是 （25） ，属于自治系统边界路由器（ASBR）的是 （26） 。




（25）A．R1　　B．R2　　C．R3　　D．R4

（26）A．R3　　B．R4　　C．R5　　D．R6

**试题（25）、（26）分析**

在这些路由器中，属于主干路由器的是 R4、R5 和 R6，同时 R6 连接外部自治系统，所以他也属于自治系统边界路由器（ASBR）。

**参考答案**

（25）D　（26）D

**试题（27）**

RIPv2 与 RIPv1 相比，它改进了什么？ （27）

（27）A．RIPv2 的最大跳数扩大了，可以适应规模更大的网络

B．RIPv2 变成无类别的协议，必须配置子网掩码

C．RIPv2 用跳数和带宽作为度量值，可以有更多的选择

D．RIPv2 可以周期性地发送路由更新，收敛速度比原来的 RIP 快

**试题（27）分析**

RIPv2 是增强了的 RIP 协议。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是 RIPv2 是一个无类别的协议（classless protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR），这些功能使得网络的设计更具伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制路由更新信息的传播。其他方面的特性与 RIPv2 相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等。

**参考答案**

（27）B

**试题（28）**

在采用 CRC 校验时，若生成多项式为 $G(X)=X^5+X^2+X+1$，传输数据为 1011110010101 时，生成的帧检验序列为＿（28）＿。

（28）A．10101　　B．01101　　C．00000　　D．11100

**试题（28）分析**

CRC 校验是数据链路层重要的差错校验技术。传输数据除以生成多项式，余数作为帧检验序列。计算过程如下：

```
                 1 0 1 0 0 1 1 1
        ________________________________
100111 | 1 0 1 1 1 1 0 0 1 0 1 0 1 0 0 0 0 0
         1 0 0 1 1 1
         -----------
             1 0 0 0 0 0
             1 0 0 1 1 1
             -----------
                   1 1 1 1 0 1
                   1 0 0 1 1 1
                   -----------
                     1 1 0 1 0 0
                     1 0 0 1 1 1
                     -----------
                       1 0 0 1 1 1
                       1 0 0 1 1 1
                       -----------
                                 0 0 0 0 0
```

**参考答案**

（28）C

**试题（29）**

结构化布线系统分为六个子系统，其中干线子系统的作用是＿（29）＿。

（29）A．连接各个建筑物中的通信系统

B．连接干线子系统和用户工作区

C．实现中央主配线架与各种不同设备之间的连接

D．实现各楼层设备间子系统之间的互连

**试题（29）分析**

在结构化布线系统中，建筑群子系统的功能是连接各个建筑物中的通信系统；连接干线子系统和用户工作区的是水平子系统；实现中央主配线架与各种不同设备之间的连接的是设备间子系统；实现各楼层设备间子系统之间的互连的是干线子系统。

**参考答案**

（29）D

**试题（30）、（31）**

Windows 命令 tracert www.163.com.cn显示的内容如下，那么本地默认网关的 IP 地址是__（30）__，网站www.163.com.cn的 IP 地址是__（31）__。

```
C:\Documents and Settings\Administrator>tracert www.163.com.cn

Tracing route to www.163.com.cn [219.137.167.157]
over a maximum of 30 hops:

  1    26 ms    15 ms    11 ms  100.100.17.254
  2    <1 ms    <1 ms    <1 ms  254-20-168-128.cos.it-comm.net [128.168.20.254]

  3    <1 ms    <1 ms    <1 ms  61.150.43.65
  4    <1 ms    <1 ms    <1 ms  222.91.155.5
  5    <1 ms    <1 ms    <1 ms  125.76.189.81
  6     1 ms    <1 ms    <1 ms  61.134.0.13
  7    28 ms    28 ms    28 ms  202.97.35.229
  8    28 ms    29 ms    29 ms  61.144.3.17
  9    29 ms    29 ms    32 ms  61.144.5.9
 10    32 ms    32 ms    32 ms  219.137.11.53
 11    29 ms    29 ms    28 ms  219.137.167.157

Trace complete.
```

（30）A．128.168.20.254　　B．100.100.17.254

C．219.137.167.157　　D．61.144.3.17

（31）A．128.168.20.254　　B．100.100.17.254

C．219.137.167.157　　D．61.144.3.17

**试题（30）、（31）分析**

tracert 命令测试到达目的所经过的各个路由器。结果中第一个为本地网关，最后一个为目的主机，故本地默认网关的 IP 地址是 100.100.17.254，网站www.163.com.cn的 IP 地址是 219.137.167.157。

**参考答案**

（30）B　（31）C

**试题（32）**

在 Linux 系统中，要查看如下输出，可使用命令__（32）__。

```
eth0 Link encap:Ethernet HWaddr 00:20:5C:00:78:33
inet addr:192.168.0.5 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9625272 errors:0 dropped:0 overruns:0 frame:0
TX packets:6997276 errors:0 dropped:0 overruns:0 frame:0
collisions:0 txqueuelen:100
interrupt:19 Base address:0xc800
```

（32）A．[root@localhost]#ifconfig
B．[root@localhost]#ipconfig eth0
C．[root@localhost]#ipconfig
D．[root@localhost]#ifconfig eth0

**试题（32）分析**

本题考查的是 Linux 网络命令的基础知识。

输出结果显示的是本地以太网接口信息，在 Linux 中，要查看本地以太网接口情况，可使用的命令是：[root@localhost]#ifconfig eth0。

**参考答案**

（32）D

**试题（33）**

当 DHCP 服务器拒绝客户端的 IP 地址请求时发送__（33）__报文。

（33）A．DhcpOffer　　B．DhcpDecline
C．DhcpAck　　D．DhcpNack

**试题（33）分析**

本题考查的是 DHCP 服务器的基础知识。

在 DHCP 客户端发送 DhcpRequest 报文后，DHCP 服务器采用 DhcpAck 报文同意客户机使用 IP 地址的请求，当 DHCP 服务器拒绝客户端的 IP 地址请求时发送 DhcpNack 报文。

**参考答案**

（33）D

**试题（34）**

在进行域名解析过程中，当主域名服务器查找不到 IP 地址时，由__（34）__负责域名解析。

（34）A．本地缓存　　B．辅域名服务器
C．根域名服务器　　D．转发域名服务器

**试题（34）分析**

本题考查的是 DNS 服务器的基础知识。

主机解析器首先查询本地缓存，查不到结果时向主域名服务器发送查询请求。主域名服务器出现故障时由辅域名服务器进行查询；当主域名服务器查找不到 IP 地址时，由转发域名服务器进行解析，转发域名服务器可以设置成互联网上任意一个 DNS 服务器，也可以是根域名服务器。

**参考答案**

（34）D

**试题（35）**

在建立 TCP 连接过程中，出现错误连接时，__（35）__标志字段置“1”。

（35）A. SYN　B. RST　C. FIN　D. ACK

**试题（35）分析**

本题考查的是 TCP 协议基础知识。

在建立 TCP 连接过程中，SYN 标志字段置“1”发生在连接请求与响应阶段；当出现错误连接时 RST 标志字段置“1”；当连接终止请求时 FIN 标志字段置“1”；ACK 标志字段置“1”表明此 TCP 段带有捎带应答。

**参考答案**

（35）B

**试题（36）、（37）**

POP3 服务器默认使用__（36）__协议的__（37）__端口。

（36）A. UDP　B. TCP　C. SMTP　D. HTTP

（37）A. 21　B. 25　C. 53　D. 110

**试题（36）、（37）分析**

本题考查的是默认端口的基础知识。

邮件服务使用两个协议，一个是 SMTP（简单邮件传送协议）和 POP3（邮局协议）协议，SMTP 协议用于发送邮件，使用 25 号端口，POP3 协议用于接收邮件，使用 110 号端口，这两种协议均是基于 TCP 协议的应用层协议。

**参考答案**

（36）B　（37）D

**试题（38）**

当客户端收到多个 DHCP 服务器的响应时，客户端会选择__（38）__地址作为自己的 IP 地址。

（38）A. 最先到达的　B. 最大的

C. 最小的　D. 租期最长的

**试题（38）分析**

本题考查的是 DHCP 的基础知识。

DHCP（Dynamic Host Configuration Protocol）协议是动态主机配置协议，基于 UDP 协议工作，用于为局域网内部的主机动态分配 IP 地址。

当局域网中存在多个 DHCP 服务器时，客户端会收到多个 DHCP 服务器的响应，此时，客户端会将第一个收到的配置响应，作为自己的 IP 地址。

**参考答案**

（38）A

**试题（39）**

在 Windows 的 DoS 窗口中输入命令

```
C:\> nslookup
> set type=a
> xyz.com.cn
```

这个命令序列的作用是<u>（39）</u>。

（39）A．查询 xyz.com.cn 的邮件服务器信息

B．查询 xyz.com.cn 到 IP 地址的映射

C．查询 xyz.com.cn 的资源记录类型

D．显示 xyz.com.cn 中各种可用的信息资源记录

**试题（39）分析**

本题考查的是 Windows 网络命令的基础知识。

nslookup 命令主要用来诊断域名系统（DNS）基础结构的信息。nslookup（name server lookup）（域名查询）：是一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。在已安装 TCP/IP 协议的电脑上面均可以使用这个命令。

该命令的使用方法如下：

```
C:\Users\HP>nslookup
默认服务器:  UnKnown
Address:  192.168.3.1
> ?
命令:   (标识符以大写表示, [] 表示可选)
NAME                    - 打印有关使用默认服务器的主机/域 NAME 的信息
NAME1 NAME2             - 同上, 但将 NAME2 用作服务器
help or ?               - 打印有关常用命令的信息
set OPTION              - 设置选项
all                     - 打印选项、当前服务器和主机
    [no]debug           - 打印调试信息
```

```
    [no]d2                       - 打印详细的调试信息
    [no]defname                  - 将域名附加到每个查询
    [no]recurse                  - 询问查询的递归应答
    [no]search                   - 使用域搜索列表
    [no]vc                       - 始终使用虚拟电路
    domain=NAME                  - 将默认域名设置为 NAME
    srchlist=N1[/N2/.../N6]      - 将域设置为 N1，并将搜索列表设置为 N1、N2 等
    root=NAME                    - 将根服务器设置为 NAME
    retry=X                      - 将重试次数设置为 X
    timeout=X                    - 将初始超时间隔设置为 X 秒
    type=X                       - 设置查询类型(如 A、AAAA、A+AAAA、ANY、CNAME、MX、
                                   NS、PTR、SOA 和 SRV)
    querytype=X                  - 与类型相同
    class=X                      - 设置查询类(如 IN (Internet)和 ANY)
    [no]msxfr                    - 使用 MS 快速区域传送
    ixfrver=X                    - 用于 IXFR 传送请求的当前版本
server NAME                      - 将默认服务器设置为 NAME，使用当前默认服务器
lserver NAME                     - 将默认服务器设置为 NAME，使用初始服务器
root                             - 将当前默认服务器设置为根服务器
ls [opt] DOMAIN [> FILE]         - 列出 DOMAIN 中的地址(可选：输出到文件 FILE)
    -a                           - 列出规范名称和别名
    -d                           - 列出所有记录
    -t TYPE                      - 列出给定 RFC 记录类型(例如 A、CNAME、MX、NS 和
                                   PTR 等)的记录
view FILE                        - 对 'ls' 输出文件排序，并使用 pg 查看
exit                             - 退出程序
```

该题目中使用了 set type a 的参数，用于查看指定域名的 IP 地址映射关系。

**参考答案**

（39）B

**试题（40）**

下面是 DHCP 协议工作的 4 种消息，正确的顺序应该是<u>（40）</u>。

① DHCP Discovery

② DHCP Offer

③ DHCP Request

④ DHCP Ack

（40）A. ①③②④　　B. ①②③④　　C. ②①③④　　D. ②③①④

**试题（40）分析**

本题考查的是 DHCP 的基础知识。

DHCP（Dynamic Host Configuration Protocol）协议是动态主机配置协议，基于 UDP 协议工作，用于为局域网内部的主机动态分配 IP 地址。

设置为自动获取 IP 地址的主机，首先以广播的形式发送 DHCP Discovery 消息，用于查找网络中的 DHCP 服务器，DHCP 服务器收到该消息后，发送 DHCP Offer 消息响应客户端，客户端再向 DHCP 服务器发送 DHCP Request 消息，以请求 IP 地址配置信息，DHCP 服务器收到请求后发送 DHCP ACK 消息确认分配 IP 地址给客户机。

**参考答案**

（40）B

**试题（41）**

在 Linux 中，__（41）__命令可将文件以修改时间顺序显示。

（41）A．ls -a　　B．ls -b　　C．ls -c　　D．ls -d

**试题（41）分析**

本题考查的是 Linux 命令的基础知识。

在 Linux 系统中，ls 命令是英文单词 list 的缩写，用于列出当前目录的内容，是 Linux 系统中用户最常用的命令之一。在目录中，ls 命令将列出其中的所有子目录与文件。对于每个文件，ls 将列出其文件名以及根据命令参数所要求的其他信息。默认情况下，输出条目按照字母顺序排列。

ls 命令的一般格式如下：

```
ls[-选项]filename | directory
```

参数如下：

-a：显示指定目录下所有子目录与文件，包括隐藏文件。

-c：按文件的修改时间顺序。

-d：如果参数是目录，只显示其名称而不显示其下的各文件。

-i：在输出的系一列显示文件的 i 节点号。

-l：以长格式来显示文件的详细信息。

**参考答案**

（41）C

**试题（42）**

要在一台主机上建立多个独立域名的站点，下面的方法中__（42）__是错误的。

（42）A．为计算机安装多块网卡　　B．使用不同的主机头名

C．使用虚拟目录　　D．使用不同的端口号

**试题（42）分析**

本题考查的是 Web 服务器构建的基础知识。

Web 网站映射多个独立域名的方法有多种，通常包括多 IP，不同的主机头以及不同

的端口号。

**参考答案**

（42）C

**试题（43）**

下面不属于数字签名作用的是___（43）___。

（43）A．接收者可验证消息来源的真实性

B．发送者无法否认发送过该消息

C．接收者无法伪造或篡改消息

D．可验证接受者的合法性

**试题（43）分析**

本题考查数字签名方面的基础知识。

数字签名用于向通信的 A、B 双方，使得 A 向 B 发送签名的消息 P，提供以下服务：

（1）B 可以验证消息 P 却是来源于 A

（2）A 不能否认发送过消息 P

（3）B 不能编造或改变消息 P

数字签名首先需要生成消息摘要，使用非对称加密算法以及私钥对摘要进行加密。接收方使用发送方的公钥对消息摘要进行验证。

**参考答案**

（43）D

**试题（44）**

下面可用于消息认证的算法是___（44）___。

（44）A．DES　　B．PGP　　C．MD5　　D．KMI

**试题（44）分析**

本题考查消息认证方面的基础知识。

认证分为实体认证和消息认证两种。实体认证是识别通信对方的身份，防止假冒，可以使用数字签名。消息认证是验证消息在传送或存储过程中有没有被篡改，通常使用报文摘要。

报文摘要是在消息后面附加一段固定长度的认证码，根据认证码检查报文是否被篡改。报文摘要是原报文唯一的压缩表示，代表了原报文的特征，也叫数字指纹。

计算报文摘要常用算法为 MD5，是由 Ronald L. Rivest 设计的一系列 Hash 函数中的第 5 个。如果更改一段明文中的一个字母，将产生不同的散列值，数据的散列值可以检验数据的完整性。

DES 是一种单密钥加密算法，PGP 是一种用于发送安全邮件的加密软件，KMI 是（Key Management Infrastructure）密钥管理基础设施，是一种适用于专用网的密钥统一集中式管理机制。

**参考答案**

（44）C

**试题（45）**

DES 加密算法的密钥长度为 56 位，三重 DES 的密钥长度为__（45）__位。

（45）A．168　　B．128　　C．112　　D．56

**试题（45）分析**

本题考查 DES 加密算法相关基础知识。

DES 加密算法使用 56 位的密钥，三重 DES 采用 2 个 DES 密钥进行 3 次加密运算，所以加密密钥的长度为 112 位。

**参考答案**

（45）C

**试题（46）**

在 Windows Server 2003 中，__（46）__组成员用户具有完全控制权限。

（46）A．Users　　B．Power Users

C．Administrators　　D．Guests

**试题（46）分析**

本题考查 Windows Server 2003 中用户组权限基础知识。

在 Windows Server 2003 中，Administrators 组中的成员用户具有完全控制权限。

**参考答案**

（46）C

**试题（47）**

SNMP 协议中网管代理使用__（47）__操作向管理站发送异步事件报告。

（47）A．trap　　B．set　　C．get　　D．get-next

**试题（47）分析**

本题考查 SNMP 协议及操作相关基础知识。

SNMP 协议中，管理站采用 get 和 get-next 操作来获取被管对象信息，采用 set 操作来设置被管对象相关参数；被管对象采用 trap 操作来向管理站发送异步事件报告。

**参考答案**

（47）A

**试题（48）**

当发现主机受到 ARP 攻击时需清除 ARP 缓存，使用的命令是__（48）__。

（48）A．arp -a　　B．arp -s　　C．arp -d　　D．arp -g

**试题（48）分析**

本题考查 ARP 协议及操作相关基础知识。

ARP 协议的功能是进行 IP 地址与 MAC 地址的映射，ARP 缓存存放的是已查询过

的记录。清除ARP缓存，使用的命令是arp -d。

**参考答案**

（48）C

**试题（49）**

从FTP服务器下载文件的命令是__（49）__。

（49）A．get　　B．dir　　C．put　　D．push

**试题（49）分析**

本题考查FTP协议及操作相关基础知识。

FTP命令由两条TCP连接来进行文件的上传和下载，FTP服务器相应也有多条命令来对应，其中从FTP服务器下载文件的命令是get。

**参考答案**

（49）A

**试题（50）**

由于内网P2P、视频/流媒体、网络游戏等流量占用过大，影响网络性能，可以采用__（50）__来保障正常的Web及邮件流量需求。

（50）A．使用网闸　　B．升级核心交换机

C．部署流量控制设备　　D．部署网络安全审计设备

**试题（50）分析**

本题考查网络规划与设计相关基础知识。

使用网闸是从物理层进行隔离，当网闸断开时所有网络应用都无法进行；升级核心交换机可以提高网络内交换的速度，但内网P2P、视频/流媒体、网络游戏等过大流量的应用仍然会影响网络性能，起不到根本作用；部署流量控制设备可以对不同的应用进行相应限制，从而降低网络堵塞；部署网络安全审计设备可对应用进行事后评估与分析，但提高不了性能。

**参考答案**

（50）C

**试题（51）**

ISP分配给某公司的地址块为199.34.76.64/28，则该公司得到的IP地址数是__（51）__。

（51）A．8　　B．16　　C．32　　D．64

**试题（51）分析**

地址块199.34.76.64/28的子网掩码为28位，只留下4位可以作为主机地址，所以该公司得到的IP地址数是16。

**参考答案**

（51）B

**试题（52）**

下面是路由表的 4 个表项，与地址 220.112.179.92 匹配的表项是__（52）__。

（52）A. 220.112.145.32/22　　B. 220.112.145.64 /22

C. 220.112.147.64/22　　D. 220.112.177.64/22

**试题（52）分析**

地址 220.112.145.32/22 的二进制形式是 **1101 1100. 0111 0000. 1001 00**01. 0010 0000

地址 220.112.145.64/22 的二进制形式是 **1101 1100. 0111 0000. 1001 00**01. 0100 0000

地址 220.112.147.64/22 的二进制形式是 **1101 1100. 0111 0000. 1001 00**11. 0100 0000

地址 220.112.177.64/22 的二进制形式是 **1101 1100. 0111 0000. 1011 00**01. 0100 0000

而地址 220.112.179.92 的二进制形式是 **1101 1100. 0111 0000. 1011 00**11. 0101 1100

所以与地址 220.112.179.92 匹配的是 220.112.177.64/22。

**参考答案**

（52）D

**试题（53）**

下面 4 个主机地址中属于网络 110.17.200.0/21 的地址是__（53）__。

（53）A. 110.17.198.0　　B. 110.17.206.0

C. 110.17.217.0　　D. 110.17.224.0

**试题（53）分析**

地址 110.17.198.0 的二进制形式是 0110 1110. 0001 0001. 1100 0110. 0000 0000

地址 110.17.206.0 的二进制形式是 **0110 1110. 0001 0001. 1100 1**110. 0000 0000

地址 110.17.217.0 的二进制形式是 0110 1110. 0001 0001. 1101 1001. 0000 0000

地址 110.17.224.0 的二进制形式是 0110 1110. 0001 0001. 1110 0000. 0000 0000

而地址 110.17.200.0/21 的二进制形式是 **0110 1110. 0001 0001. 1100 1**000. 0000 0000

所以与地址 110.17.200.0/21 匹配的是 110.17.206.0。

**参考答案**

（53）B

**试题（54）、（55）**

某用户得到的网络地址范围为 110.15.0.0～110.15.7.0，这个地址块可以用__（54）__表示，其中可以分配__（55）__个可用主机地址。

（54）A. 110.15.0.0/20　　B. 110.15.0.0/21

C. 110.15.0.0/16　　D. 110.15.0.0/24

（55）A. 2048　　B. 2046　　C. 2000　　D. 2056

**试题（54）、（55）分析**

网络地址块 110.15.0.0～110.15.7.0 可以用 110.15.0.0/21 表示，用于分配 IP 地址的代码占 11 位，除过全 0 的网络地址和全 1 的广播地址外，共有 2046 个主机地址。

**参考答案**

（54）B （55）B

**试题（56）**

下面的提示符__（56）__表示特权模式。

（56）A．> B．# C．（config）# D．!

**试题（56）分析**

交换机的各种提示符如下：

Switch> （用户执行模式）

Switch # （特权模式）

Switch(config)# （配置模式）

**参考答案**

（56）B

**试题（57）**

把路由器当前配置文件存储到 NVRAM 中的命令是__（57）__。

（57）A．Router(config)#copy current to starting

B．Router#copy starting to running

C．Router(config)#copy running-config starting-config

D．Router#copy run startup

**试题（57）分析**

把路由器当前配置文件存储到 NVRAM 中的命令是 Router#copy run startup。

**参考答案**

（57）D

**试题（58）**

如果路由器显示“Serial 1 is down, line protocol is down”故障信息，则问题出在 OSI 参考模型的__（58）__。

（58）A．物理层 B．数据链路层 C．网络层 D．会话层

**试题（58）分析**

1．Serial 1 is up，line protocol is up，工作正常；

2．Serial 1 is down，line protocol is down，故障原因是传输线路不通、连接线未连接或连接错误，问题出在物理层；

3．Serial 1 is up，line protocol is down，错误原因是本地或远程配置错，需要进行端口本地自环测试。

**参考答案**

（58）A

**试题（59）**

下面的交换机命令中__（59）__为端口指定 VLAN。

（59）A．S1(config-if)# vlan-menbership static

B．S1(config-if)# vlan database

C．S1(config-if)# switchport mode access

D．S1(config-if)# switchport access vlan 1

**试题（59）分析**

为端口指定 VLAN 的交换机命令是 S1(config-if)# switchport access vlan 1，为本地端口指定访问 vlan 1。

**参考答案**

（59）D

**试题（60）**

STP 协议的作用是__（60）__。

（60）A．防止二层环路　　B．以太网流量控制

C．划分逻辑网络　　D．基于端口的认证

**试题（60）分析**

生成树协议（Spanning Tree Protocol，STP）是为了防止通过网桥或交换机连接的局域网出现环路，这种情况使得一个网站既出现在网桥的这一边，又出现在网桥的另一边，从而无法进行有效的帧转发。通过 STP 协议，阻塞了网桥的部分端口，使得通过网桥互连的局域网形成一个生成树，这样就不会出现环路了。

**参考答案**

（60）A

**试题（61）**

VLAN 之间通信需要__（61）__的支持。

（61）A．网桥　　B．路由器　　C．VLAN 服务器　　D．交换机

**试题（61）分析**

一个 VLAN 就是一个广播域，VLAN 内部通过交换机互相通信，VLAN 之间互相通信需要通过路由器进行转发。

**参考答案**

（61）B

**试题（62）**

以太网中出现冲突后，发送方什么时候可以再次尝试发送？__（62）__

（62）A．再次收到目标站的发送请求后

B．在 JAM 信号停止并等待一段固定时间后

C．在 JAM 信号停止并等待一段随机时间后

D．当 JAM 信号指示冲突已经被清除后

**试题（62）分析**

按照以太网的 CSMA/CD 协议，如果网络中出现冲突，试图发送的一方先要发送阻塞信号 JAM，在阻塞信号停止后运行二进程指数后退算法，这种算法使得后退时延的取值范围与重发次数 n 形成二进制指数关系。或者说，随着重发次数 n 的增加，后退时延 $t_\xi$的取值范围按 2 的指数增大。即第一次试发送时 n 的值为 0，每冲突一次 n 的值加 1，并按下式计算后退时延。

$$\begin{cases} \xi=\text{random}[0，2^n] \\ t_\xi=\xi\tau \end{cases}$$

其中，第一式是在区间[0，$2^n$]中取一均匀分布的随机整数$\xi$，第二式是计算出随机后退时延。为了避免无限制的重发，要对重发次数 n 进行限制，这种情况往往是信道故障引起的。通常当 n 增加到某一最大值（例如 16）时，停止发送，并向上层协议报告发送错误。

由于$\xi$是一个随机数，所以 $t_\xi$也是一段随机的时间。但这种随机性是与重发次数 n 相关的。n 越大，这一段随机时间的也越长。

**参考答案**

（62）C

**试题（63）、（64）**

网桥怎样知道网络端口连接了哪些网站？__（63）__。当网桥连接的局域网出现环路时怎么办？__（64）__

（63）A．如果从端口收到一个数据帧，则将其目标地址记入该端口的数据库

B．如果从端口收到一个数据帧，则将其源地址记入该端口的数据库

C．向端口连接的各个站点发送请求以便获取其 MAC 地址

D．由网络管理员预先配置好各个端口的地址数据库

（64）A．运行生成树协议阻塞一部分端口

B．运行动态主机配置协议重新分配端口地址

C．通过站点之间的协商产生一部分备用端口

D．各个网桥通过选举产生多个没有环路的生成树

**试题（63）、（64）分析**

网桥查看每个端口出现的帧，将其源地址记入该端口的数据库，这样就可以了解各个端口连接了哪些网站。当网桥连接的局域网出现环路时，所有的网桥通过运行生成树协议，阻塞一部分端口，使得不再出现环路。

**参考答案**

（63）B （64）A

**试题（65）**

IEEE 802.11 标准采用的工作频段是__（65）__。

（65）A．900MHz 和 800MHz　　B．900MHz 和 2.4GHz

C．5GHz 和 800MHz　　D．2.4GHz 和 5GHz

**试题（65）分析**

IEEE 802.11 标准采用的工作频段是 2.4GHz 和 5GHz。

**参考答案**

（65）D

**试题（66）**

IEEE 802.11 MAC 子层定义的竞争性访问控制协议是__（66）__。

（66）A．CSMA/CA　　B．CSMA/CB

C．CSMA/CD　　D．CSMA/CG

**试题（66）分析**

IEEE 802.11 MAC 子层定义的竞争性访问控制协议是 CSMA/CA，即载波监听、多路访问、冲突避免协议。

**参考答案**

（66）A

**试题（67）**

无线局域网的新标准 IEEE 802.11n 提供的最高数据速率可达到__（67）__Mb/s。

（67）A．54　　B．100　　C．200　　D．300

**试题（67）分析**

无线局域网的新标准 IEEE 802.11n 提供的最高数据速率可达到 300Mb/s。

**参考答案**

（67）D

**试题（68）**

在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是__（68）__。

（68）A．设备防雷击　　B．入侵检测

C．漏洞发现与补丁管理　　D．流量控制

**试题（68）分析**

设备防雷击属于物理线路安全措施，入侵检测和流量控制属于网络安全措施，漏洞发现与补丁管理属于系统安全措施。

**参考答案**

（68）C

**试题（69）**

在网络的分层设计模型中，对核心层工作规程的建议是__（69）__。

（69）A. 要进行数据压缩以提高链路利用率
B. 尽量避免使用访问控制列表以减少转发延迟
C. 可以允许最终用户直接访问
D. 尽量避免冗余连接

**试题（69）分析**

层次局域网结构根据功能要求不同将局域网划分为核心层、汇聚层和接入层。这些层次的主要区别是：

（1）核心层实现高速数据转发。

（2）汇聚层实现丰富的接口和接入层之间的互访控制。

（3）接入层实现用户接入。

所以核心层要尽量避免使用访问控制列表以减少转发延迟。

**参考答案**

（69）B

**试题（70）**

在网络规划和设计过程中，选择网络技术时要考虑多种因素。下面的各种考虑中不正确的是__（70）__。

（70）A. 网络带宽要保证用户能够快速访问网络资源
B. 要选择具有前瞻性的网络新技术
C. 选择网络技术时要考虑未来网络扩充的需要
D. 通过投入产出分析确定使用何种技术

**试题（70）分析**

在网络规划和设计过程中，需要足够的网络带宽来保证用户能够快速访问网络资源，选择网络技术时要考虑未来网络扩充的需要，进而通过投入产出分析确定使用何种技术。是否采用前瞻性的网络新技术需看是否满足设计需求。

**参考答案**

（70）B

**试题（71）～（75）**

All three types of cryptography schemes have unique function mapping to specific applications. For example, the symmetric key__（71）__approach is typically used for the encryption of data providing__（72）__, whereas asymmetric key cryptography is mainly used in key__（73）__and nonrepudiation, thereby providing confidentiality and authentication. The hash__（74）__(noncryptic), on the other hand, does not provide confidentiality but provides message integrity, and cryptographic hash algorithms provide message__（75）__and identity of

peers during transport over insecure channels.

（71）A. cryptography　B. decode　C. privacy　D. security
（72）A. conduction　B. confidence　C. confidentiality　D. connection
（73）A. authentication　B. structure　C. encryption　D. exchange
（74）A. algorithm　B. secure　C. structure　D. encryption
（75）A. confidentiality　B. integrity　C. service　D. robustness

**参考译文**

所有三种加密方案都以其独特的功能对应于具体的应用。例如，对称密钥加密方案通常用于保密数据的加密，而非对称加密主要用于密钥交换和非否认验证，从而提供了保密性和认证机制。另一方面，哈希算法（非加密的）不能提供保密性，但可以提供报文完整性检测，而加密的哈希算法还可以提供报文完整性和对等方的标识验证，这在通过不安全信道传输的过程中是有用的。

**参考答案**

（71）A　（72）C　（73）D　（74）A　（75）B

# 第 32 章　2016 下半年网络工程师下午试题分析与解答

**试题一（共 20 分）**

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

**【说明】**

某企业的行政部、技术部和生产部分布在三个区域，随着企业对信息化需求的提高，现拟将网络出口链路由单链路升级为双链路，提升 ERP 系统服务能力以及加强员工上网行为管控。网络管理员依据企业现有网络和新的网络需求设计了该企业网络拓扑图 1-1，并对网络地址重新进行了规划，其中防火墙设备集成了传统防火墙与路由功能。

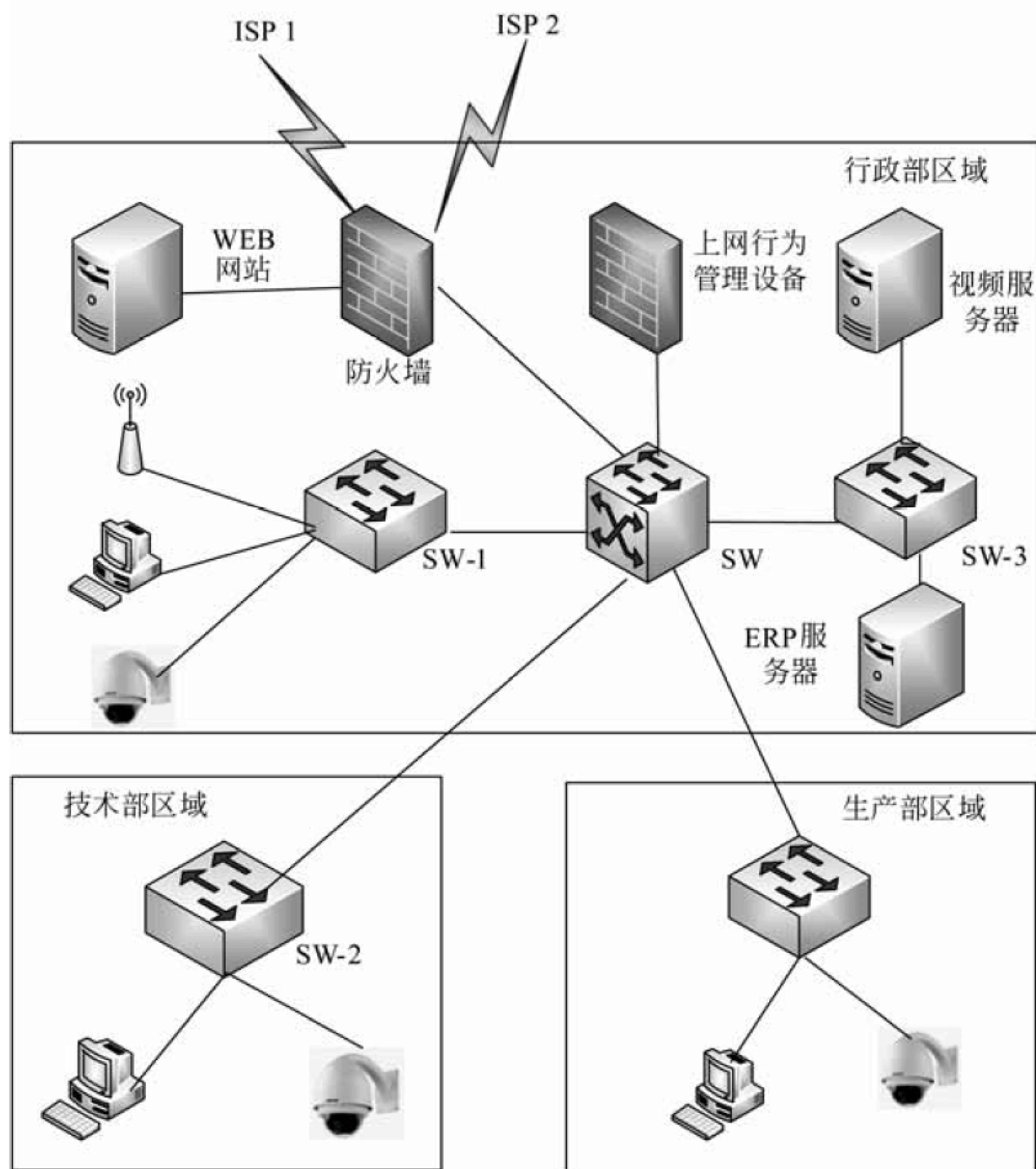



图 1-1

**【问题 1】（4 分）**

在图 1-1 的防火墙设备中，配置双出口链路有提高总带宽、____（1）____、链路负载均衡作用。通过配置链路聚合来提高总带宽，通过配置____（2）____来实现链路负载均衡。

**【问题 2】（4 分）**

防火墙工作模式有路由模式、透明模式、混合模式，若该防火墙接口均配有 IP 地址，则防火墙工作在____（3）____模式，该模式下，ERP 服务器部署在防火墙的____（4）____区域。

**【问题 3】（4 分）**

若地址规划如表 1-1 所示，从 IP 规划方案看该地址的配置可能有哪些方面的考虑？

**表 1-1**

| 位置或系统 | VLAN ID | 地 址 区 间 | 信息点数量 | 备　注 |
|---|---|---|---|---|
| 行政部 | 10～13 | 192.168.10.0～192.168.13.0 | 60 | 网段按楼层分配，每个网段末位地址为网关 |
| 技术部 | 14～17 | 192.168.14.0～192.168.17.0 | 80 | |
| 生产部 | 18～20 | 192.168.18.0～192.168.20.0 | 30 | |
| 无线网络 | 22 | 192.168.22.0 | | 行政楼区域部署 |
| 监控网络 | 23 | 192.168.23.0 | 30 | 信息点分散 |
| ERP | 30 | 192.168.30.0 | | |

**【问题 4】（3 分）**

该网络拓扑中，上网行为管理设备的位置是否合适？请说明理由。

**【问题 5】（3 分）**

该网络中有无线节点的接入，在安全管理方面应采取哪些措施？

**【问题 6】（2 分）**

该网络中视频监控系统与数据业务共用网络带宽，存在哪些弊端？

**试题一分析**

本题考查企业网络的规划相关知识，包括网络接入策略、网络拓扑规划、服务器以及网络安全设备部署等的综合应用。

此类题目要求考生具备较为丰富的网络构建经验，具有对题目给出的网络环境进行分析的能力，对于题目给出的某企业网络的应用，进行分析并说明该网络部署的依据。

**【问题 1】**

在本问题中，防火墙部署在企业网的出口，起到了安全隔离内部网与外部网的作用，当两条 ISP 链路接入防火墙时，可以起到提高总带宽、链路冗余和负载均衡的作用。一般而言，增加出口链路数量必然会增加企业网的出口总带宽，降低网络拥塞，避免网络瓶颈的出现。两条链路也可以起到链路冗余的作用，当一条链路不可用或者异常中断时，故障链路上的数据可以自动的切换到正常链路之上，可以避免业务的中断。通过策略路由对网络请求进行重定向和内容管理，实现数据在两条链路上的负载均衡。

【问题 2】

防火墙有三种模式选择：路由模式、透明模式、混合模式。如果防火墙接口配置有 IP 地址并通过第三层对外连接，则认为防火墙工作在路由模式下；若防火墙接口未配置 IP 地址并通过第二层对外连接，则防火墙工作在透明模式下；若防火墙同时具有工作在路由模式（某些接口具有 IP 地址）和透明模式的接口（某些接口无 IP 地址），则防火墙工作在混合模式下。

防火墙位于内、外网之间时，防火墙分为三个区域，外部网络、内部网络以及 DMZ 区域。在该模式下，ERP 服务器部署在防火墙的内部区域，用于内部用户访问，该服务器对外不提供访问服务，确保了内部数据的安全性。Web 网站对外部用户和内部用户同时提供服务，应该部署在防火墙的 DMZ 区域。

【问题 3】

从表 1-1 可知，该企业的地址规划从地理区域和业务两个方面进行了考虑。给处于相同地理区域的部门分配同一个网段的 IP 地址，便于配置相同的安全策略，易于网络故障的排查与维护。给分散在不同地理位置的监控业务划分在同一个 IP 网段，通过 VLAN 组网，使用固定的 IP 地址，便于灵活管理。

【问题 4】

上网行为管理设备是对用户使用互联网进行管理和控制的设备，该设备可以实现对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析等功能。此类设备在网络的部署通常都提供串接和旁路方式，都可以实现对上网行为的管控。

【问题 5】

该网络在无线节点的接入可以采取的安全策略包括与其他内部网络进行逻辑隔离，对无线终端接入进行认证，对无线接入的访问权限进行授权等等多种方式。

【问题 6】

该网络中的视频监控系统与数据业务共享带宽，主要的弊端有两个方面，一是视频监控数据量较大并且始终占用一定量的带宽资源，会影响业务数据。二是视频监控系统未做安全防范部署说明，在内部网络中存在数据泄露风险。

**参考答案**

【问题 1】

（1）提高链路冗余或可靠性

（2）策略路由或路由策略

【问题 2】

（3）路由

（4）内部

【问题 3】

用户上网 IP 的划分按地理位置划分，便于维护和网络安全管理；监控按业务类型独

立划分 VLAN，使用固定 IP，便于灵活管理。

【问题 4】

合适，该设备有串接和旁路等多种方式，均可实现上网行为管控。

【问题 5】

1．配置单独 VLAN

2．终端接入认证

3．访问权限控制

【问题 6】

1．视频数据会占用较多网络带宽，影响业务数据传输速率。

2．视频监控系统未做安全防范，存在一定数据泄漏风险。

**试题二（共 20 分）**

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

图 2-1 是某互联网企业网络拓扑，该网络采用二层结构，网络安全设备有防火墙、入侵检测系统，楼层接入交换机 32 台，全网划分 17 个 VLAN，对外提供 Web 和邮件服务，数据库服务器和邮件服务器均安装 CentOS 操作系统（Linux 平台），Web 服务器安装 Windows 2008 操作系统。

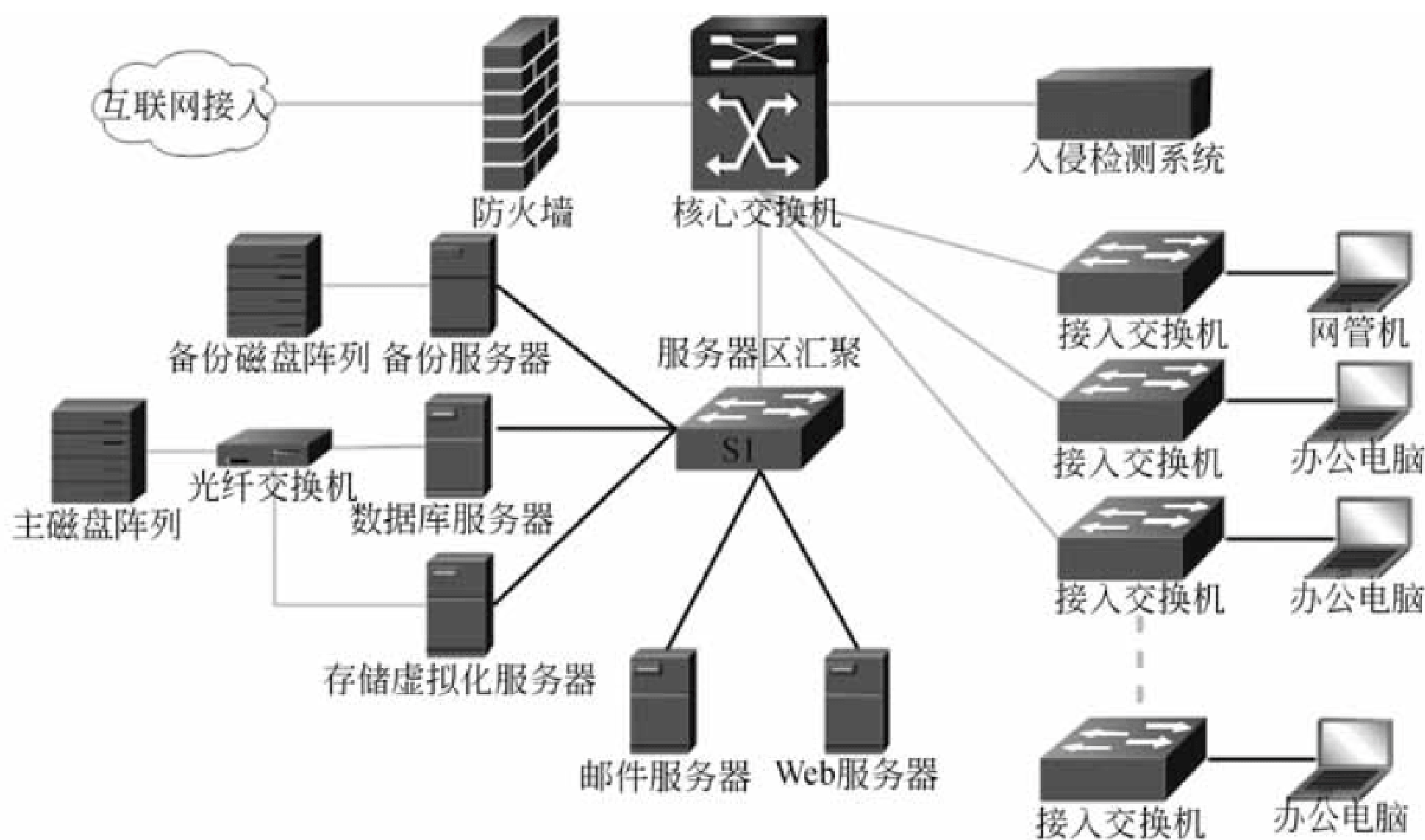



图 2-1

【问题 1】（6 分）

SAN 常见方式有 FC-SAN 和 IP SAN，在图 2-1 中，数据库服务器和存储设备连接方式为__（1）__，邮件服务器和存储设备连接方式为__（2）__。

虚拟化存储常用文件系统格式有 CIFS、NFS，为邮件服务器分配存储空间时应采用的文件系统格式是__（3）__，为 Web 服务器分配存储空间应采用的文件系统格式是__（4）__。

**【问题 2】（3 分）**

该企业采用 RAID5 方式进行数据冗余备份。请从存储效率和存储速率两个方面比较 RAID1 和 RAID5 两种存储方式，并简要说明采用 RAID5 存储方式的原因。

**【问题 3】（8 分）**

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断：

1．通过网管机，利用__（5）__登录到邮件服务器，发现邮件服务正常，但是连接时断时续。

2．使用__（6）__命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区汇聚交换机 S1，发现连接邮件服务器的端口数据流量异常，收发包量很大。

3．根据以上情况，邮件服务器的可能故障为__（7）__，应采用__（8）__的办法处理上述故障。

（5）A．ping　　B．ssh　　C．tracert　　D．mstsc

（6）A．ping　　B．telnet　　C．tracet　　D．netstat

（7）A．磁盘故障　　B．感染病毒　　C．网卡故障　　D．负荷过大

（8）A．更换磁盘　　B．安装防病毒软件，并查杀病毒

　　C．更换网卡　　D．提升服务器处理能力

**【问题 4】（3 分）**

上述企业网络拓扑存在的网络安全隐患有：__（9）__、__（10）__、__（11）__。

（9）～（11）备选答案：

A．缺少针对来自局域网内部的安全防护措施

B．缺少应用负载均衡

C．缺少流量控制措施

D．缺少防病毒措施

E．缺少 Web 安全防护措施

F．核心交换机到服务器区汇聚交换缺少链路冗余措施

G．VLAN 划分太多

**试题二分析**

本题考查存储系统和网络安全的基本知识。

此类题目要求考生熟悉常用 RAID 方式的优缺点，熟练运用网络故障诊断的常用命令和方法，了解网络安全防范的基础知识。要求考生具有网络管理、故障诊断和解决问题的实践经验。

**【问题 1】**

本问题中，数据库服务器通过光纤交换机与存储设备（即：主磁盘阵列）连接，采

用 FC 光纤通道传输，故连接方式为 FC-SAN；邮件服务器通过服务器区汇聚交换机连接到存储虚拟化，采用 IP 网络传输，故连接方式为 IP-SAN。

CIFS、NFS 为网络文件系统的两种常用协议，CIFS 常用于 Windows 系统，NFS 常用 Linux 系统。

**【问题 2】**

RAID1 是一种镜像存储阵列，存储数据时，将一块磁盘的内容完全复制到另一块磁盘上，进行 100%的完全备份，数据可靠性、安全性高，但是，磁盘空间利用率低，如 N 块磁盘构建的 RAID1 阵列只能有 N/2 块磁盘的容量，存储成本高，写数据时需要同时写入到两块磁盘并做比较，所以写效率低。

RAID5 是一种分布式奇偶校验存储阵列，将磁盘进行条带化分割，相同的条带区进行奇偶校验（异或运算），校验数据平均分布在每块磁盘上。如 N 块磁盘构建的 Raid 5 阵列有 N-1 块磁盘的容量，磁盘空间利用率非常高，且数据安全、读写速度快，为目前应用最为广泛的 RAID 技术。其缺点是当其中一块磁盘故障，读写性能会下降很多，实际应用中，发现磁盘故障应及时更换。

**【问题 3】**

邮件服务器为 Linux 系统，远程连接一般采用 SSH 连接登录，同时，使用 Ping 命令，诊断邮件服务器的网络连通性和丢包情况，本例故障表现为邮件服务器丢包严重并且连接该服务器的交换机接口流量异常，一般原因为感染病毒、感染木马等，造成服务器对外发包异常，结合备选答案，应选感染病毒，应对措施为病毒查杀。

**【问题 4】**

本例中，只在网络出口处部署防火墙，而内部用户与服务器区未做任何安全防范措施，建议在服务器区汇聚交换机与核心交换机之间部署网络安全设备，防范来自内部局域网的网络安全隐患。从问题 3 中，可以看出，部分服务器未安装杀毒软件，应尽快安装杀毒软件。该企业对外提供 Web 服务，但是未做 Web 安全的相关防范措施，建议增加 IPS 或者 WAF 等安全设备。结合备选答案，应选 A、D、E。

**参考答案**

**【问题 1】**

（1）FC-SAN

（2）IP-SAN

（3）NFS

（4）CIFS

**【问题 2】**

1．RAID1 的磁盘利用率为 n/2，读写性能较低。

2．RAID5 的磁盘利用率为 n−1，读写性能高。

**【问题 3】**

（5）B

（6）A

（7）B

（8）B

【问题 4】

（9）A

（10）D

（11）E

注：（9）、（10）、（11）答案不分先后顺序

**试题三（共 20 分）**

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司的 IDC（互联网数据中心）服务器 Server1 采用 Windows Server 2003 操作系统，IP 地址为 172.16.145.128/24，为客户提供 Web 服务和 DNS 服务；配置了三个网站，域名分别为 www.company1.com、www.company2.com 和 www.company3.com，其中 company1 使用默认端口。基于安全的考虑，不允许用户上传文件和浏览目录。company1.com、company2.com 和 company3.com 对应的网站目录分别为 company1-web、company2-web 和 company3-web，如图 3-1 所示。

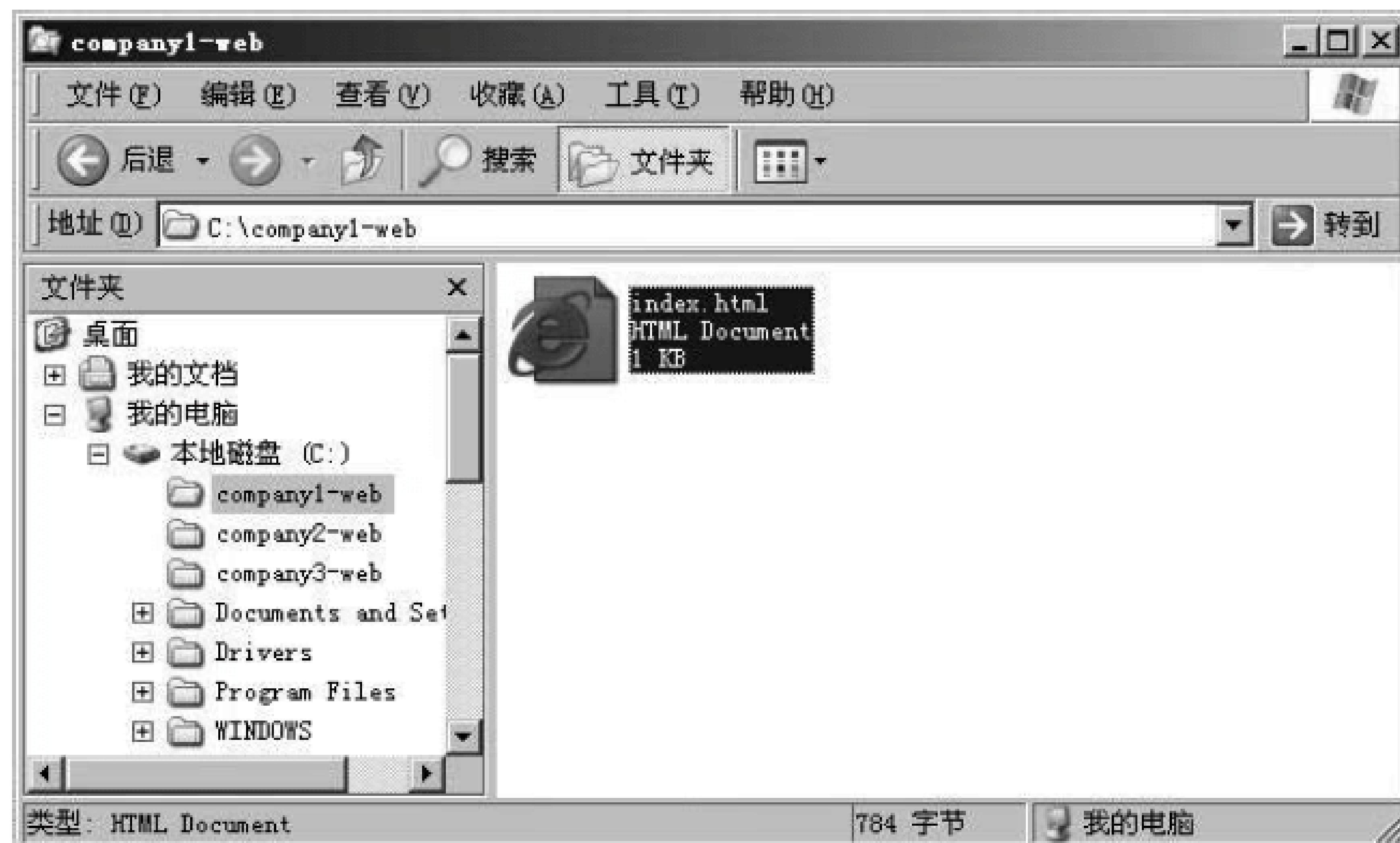



图 3-1

【问题 1】（2 分，每空 1 分）

为安装 Web 服务和 DNS 服务，Server1 必须安装的组件有__（1）__和__（2）__。

（1）、（2）备选答案：

A. 网络服务　B. 应用程序服务器　C. 索引服务　D. 证书服务　E. 远程终端

【问题 2】（4 分，每空 2 分）

在 IIS 中创建这三个网站时，在图 3-2 中勾选读取、__（3）__和执行。并在图 3-3 所示的文档选项卡中添加__（4）__为默认文档。

**【问题 3】（6 分，每空 1 分）**

1．为了节省成本，公司决定在一台计算机上为多类用户提供服务。使用不同端口号来区分不同网站，company1 使用默认端口＿（5）＿，company2 和 company3 的端口应在 1025 至＿（6）＿范围内任意选择，在访问 company2 或者 company3 时需在域名后添加对应端口号，使用＿（7）＿符号连接。设置完成后，管理员对网站进行了测试，测试结果如图 3-4 所示，原因是＿（8）＿。

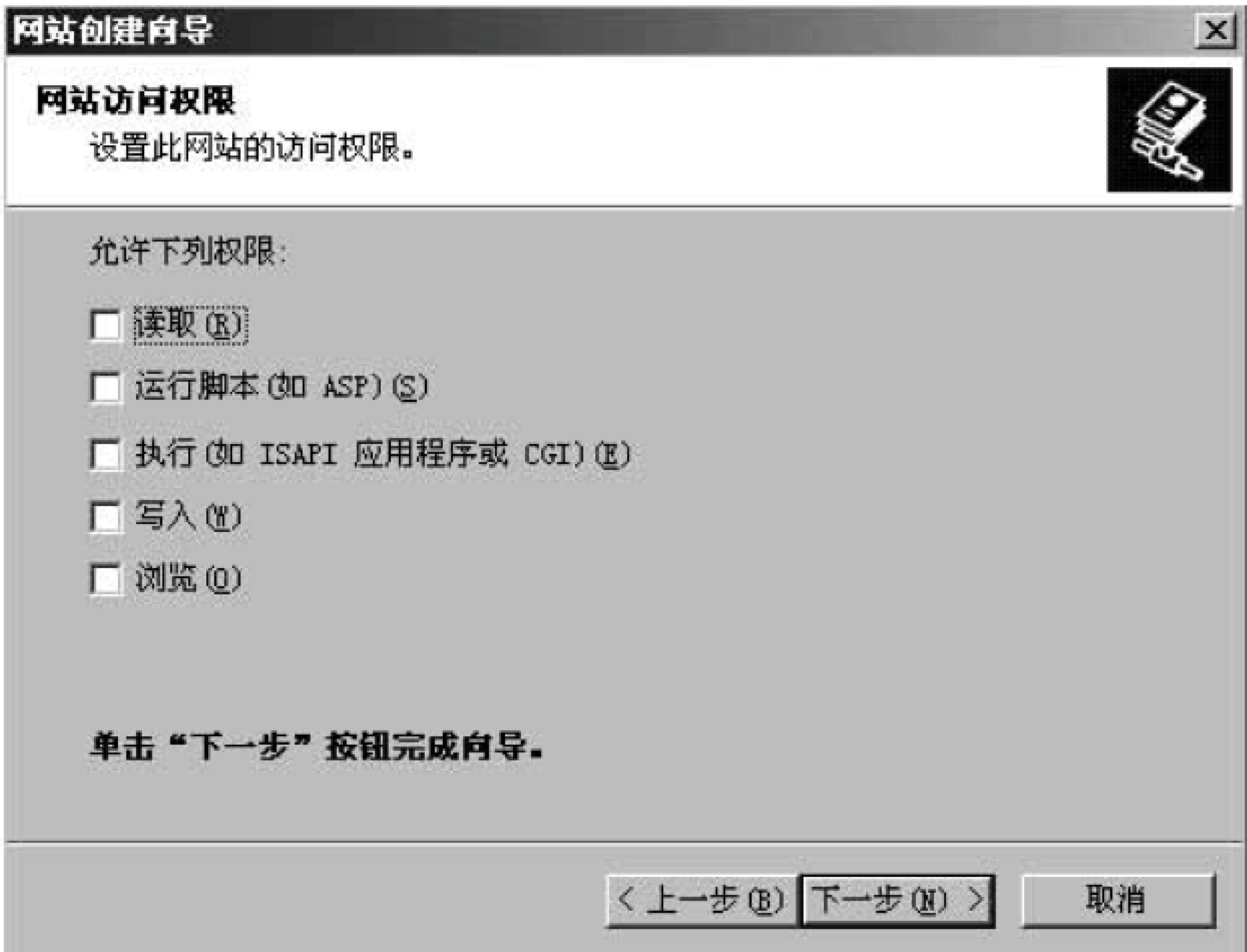



图 3-2




图 3-3

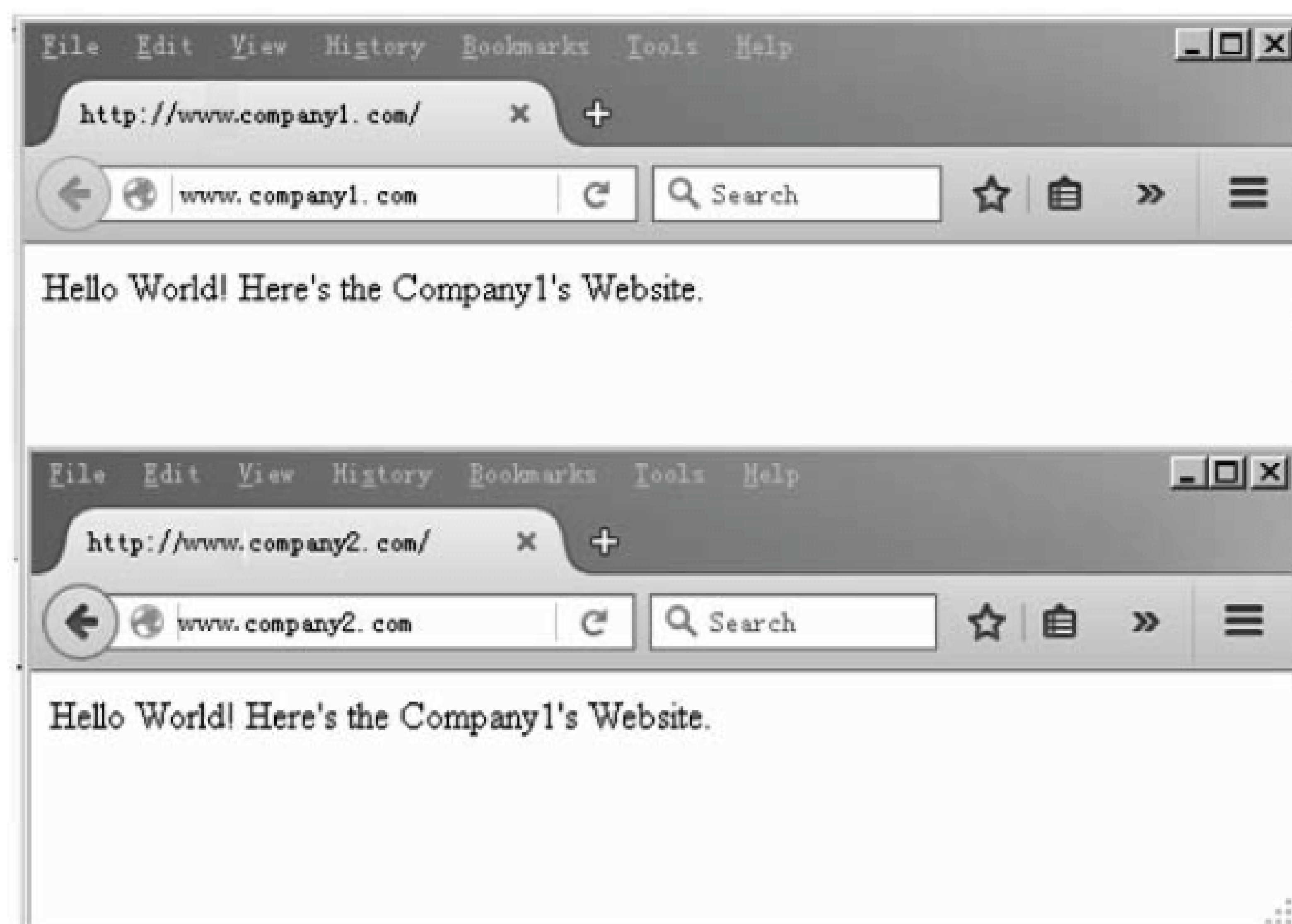



图 3-4

（8）备选答案：

A．IP 地址对应错误　　　　　B．未指明 company1 的端口号

C．未指明 company2 的端口号　D．主机头设置错误

2．为便于用户访问，管理员决定采用不同主机头值的方法为用户提供服务，需在 DNS 服务中正向查找区域为三个网站域名分别添加＿（9）＿记录。网站 company2 的主机头值应设置为＿（10）＿。

**【问题 4】（8 分，每空 2 分）**

随着 company1 网站访问量的不断增加，公司为 company1 设立了多台服务器。下面是不同用户 ping 网站 www.company1.com 后返回的 IP 地址及响应状况，如图 3-5 所示。

```
Microsoft Windows [版本 5.2.3790]
 (c) 版权所有 1985-2003 Microsoft Corp.

C:\Users>ping www.company1.com

Pinging company1.wscache.ourglb0.com [172.16.145.192] with 32 bytes of data:

Reply from 172.16.145.192: bytes=32 time=11ms TTL=57
Reply from 172.16.145.192: bytes=32 time=13ms TTL=57
Reply from 172.16.145.192: bytes=32 time=15ms TTL=57
Reply from 172.16.145.192: bytes=32 time=13ms TTL=57

Ping statistics for 172.16.145.192:
    Packets: Sent=4, Received=4, Lost=0 <0% loss>,
Approximate round trip times in milli-seconds:
    Minimum=11ms, Maximum=15ms, Average=13ms
```

```
Microsoft Windows [版本 10.0.10586]
 (c) 2015 Microsoft Corporation.

C:\Users>ping www.company1.com

Pinging company1.wscache.ourglb0.com [172.16.145.193] with 32 bytes of data:

Reply from 172.16.145.193: bytes=32 time=5ms TTL=57
Reply from 172.16.145.193: bytes=32 time=6ms TTL=57
Reply from 172.16.145.193: bytes=32 time=5ms TTL=57
Reply from 172.16.145.193: bytes=32 time=8ms TTL=57

Ping statistics for 172.16.145.193:
Packets: Sent=4, Received=4, Lost=0 <0% loss>,
Approximate round trip times in milli-seconds:
Minimum=5ms, Maximum=8ms, Average=6ms
```

图 3-5

从图 3-5 可以看出，域名 www.company1.com 对应了多个 IP 地址，说明在图 3-6 所示的 DNS 属性中启用了＿（11）＿功能。

在图 3-6 中勾选了“启用网络掩码排序”后，当存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 的网络掩码匹配度，按照＿（12）＿原则来应答客户端的解析请求。如果勾选了“禁用递归”，这时 DNS 服务器仅采用＿（13）＿查询模式。当同时启用了网络掩码排序和循环功能时，＿（14）＿优先级较高。

（14）备选答案：

A．循环　　　　B．网络掩码排序




图 3-6

## 试题三分析

本题考查 Windows Server 2003 服务器的基本配置和基本功能等相关知识。

此类题目要求考生掌握 IIS、DNS 和 Web 服务器基本参数的配置、基本命令和基本功能等相关知识，属传统考题。

**【问题 1】**

为安装 DNS 服务和 Web 服务，Server1 必须安装的组件有网络服务和应用程序服务器，“域名系统（DNS）”是“网络服务”中的一个组件，“Internet 信息服务（IIS）”是“应用程序服务器”中的一个组件。

**【问题 2】**

在 IIS 中创建网站，必须运行网页脚本，因此需要在网站访问权限中勾选“运行脚

本”。由图 3-1 可知网站目录中的文档名为 index.html，因此必须在图 3-3 所示的网站属性的文档选项卡中添加 index.html 作为默认文档。

【问题 3】

1. TCP 协议为端口号标志分配了 16 位，一共可允许 65535 个不同的端口号。公认端口（熟知端口）号从 0 到 1023，它们紧密绑定于一些服务，通常这些端口的通信明确表明了某种服务的协议，如 HTTP 的默认端口号就是 80。从 1024 到 65535 的端口号又分为两类，可以作为自由选择的端口号使用。由于 company2 和 company3 没有使用默认端口号 80，因此在访问这两个网站时，必须在域名后添加端口号，并用“:”连接。图 3-4 所示是输入了 company2 的域名而访问的是 company1 的网站，就是因为没有在 company2 的域名后添加端口号，此时会认为端口号是默认端口 80。

2. 一般 Web 服务器一个 IP 地址的 80 端口只能正确对应一个网站，处理一个域名的访问请求。Web 服务器在不使用多个 IP 地址和端口的情况下，如果需要支持多个相对独立的网站就需要一种机制来分辨同一个 IP 地址上的不同网站的请求，这就出现了主机头绑定的方法。此时需要在 DNS 服务中的正向查找区域为三个网站域名添加主机（A）记录，并将每个 company 的主机头值设置为它的域名。

【问题 4】

DNS 属性中启用“循环”功能后，同一个域名可以对应多个 IP 地址。当启用“网络掩码排序”功能后，如果存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 地址的网络掩码匹配度，按照最长匹配的原则来应答客户端的解析请求。

DNS 查询模式有递归查询和迭代查询，当在 DNS 属性中勾选了“禁用递归”时，DNS 服务器就会采用迭代查询模式。如果同时启用了“网络掩码排序”和“循环”功能时，网络掩码排序的优先级较高。

**参考答案**

【问题 1】

（1）A

（2）B

【问题 2】

（3）运行脚本

（4）index.html

【问题 3】

1.（5）80 （6）65535 （7）: 或者 冒号 （8）C

2.（9）主机（A） （10）www.company2.com

【问题 4】

（11）循环

（12）最长匹配

（13）迭代

（14）B

**试题四（共 15 分）**

阅读以下说明，回答问题 1 至问题 2，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司建立局域网拓扑图如图 4-1 所示。公司计划使用路由器作为 DHCP 服务器，根据需求，公司内部使用 C 类地址段，服务器地址段为 192.168.2.0/24，S2 和 S3 分别为公司两个部门的接入交换机，分别配置 VLAN 10 和 VLAN 20，地址段分别使用 192.168.10.0/24 和 192.168.20.0/24，通过 DHCP 服务器自动为两个部门分配 IP 地址，地址租约期为 12 小时。其中，192.168.10.1～192.168.10.10 作为保留地址。

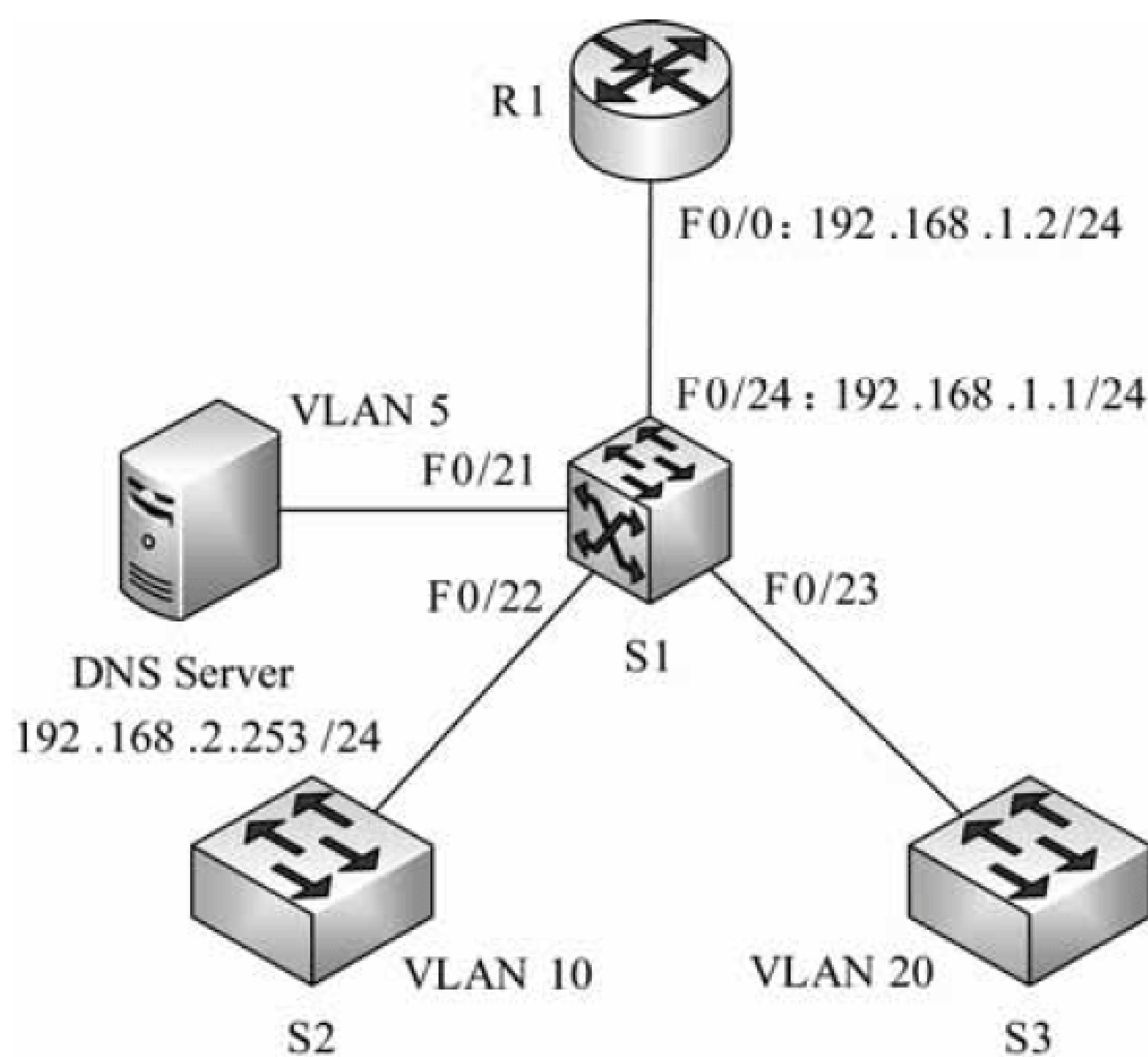



图 4-1

**【问题 1】（10 分，每空 1 分）**

下面是 R1 的配置代码，请将下面配置代码补充完整。

```
R1#config t
R1 (config)# interface FastEthernet0/0
R1 (config-if)#ip address  (1)   (2)
R1 (config-if)#no shutdown
R1(config-if)#exit
R1 (config)#ip dhcp  (3)  depart1
R1 (dhcp-config)#network 192.168.10.0 255.255.255.0
R1 (dhcp-config)#default-router 192.168.10.254 255.255.255.0
R1 (dhcp-config)#dns-server  (4)
```

```
R1 (dhcp-config)#lease 0 __(5)__ 0
R1 (dhcp-config)#exit
R1 (config)#ip dhcp pool depart2
R1(dhcp-config)# network __(6)__ __(7)__
R1 (dhcp-config)#default-router 192.168.20.254 255.255.255.0
R1 (dhcp-config)# dns-server 192.168.2.253
R1 (dhcp-config)# lease 0 12 0
R1 (dhcp-config)#exit
R1 (config)# ip dhcp excluded-address __(8)__ __(9)__
R1 (config)# ip dhcp excluded-address __(10)__  //排除掉不能分配的 IP 地址
R1 (config)# ip dhcp excluded-address 192.168.20.254
......
```

**【问题 2】（5 分，每空 1 分）**

下面是 S1 的配置代码，请将下面配置代码或解释补充完整。

```
S1#config terminal
S1(config)#interface vlan 5
S1(config-if)#ip address 192.168.2.254 255.255.255.0
S1(config)#interface vlan 10
S1(config-if)#ip helper-address __(11)__         //指定 DHCP 服务器的地址
S1(config-if)#exit
S1(config)#interface vlan 20
......
S1(config)#interface f0/24
S1(config-if)#switchport mode __(12)__
S1(config-if)# switchport trunk __(13)__ vlan all  //允许所有 VLAN 数据通过
S1(config-if)#exit
S1(config)#interface f0/21
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 5
S1(config-if)#exit
S1(config)#interface f0/22
S1(config-if)#switchport mode access
S1(config-if)#switchport access__(14)__
S1(config)#interface f0/23
S1(config-if)#switchport mode access
S1(config-if)#switchport access__(15)__
```

## 试题四分析

本题考查考生对交换机和路由器基本配置知识的掌握和应用。

该类题目要求考生首先详细阅读题干，清楚题目的要求和意图，题目要求为公司网络配置 DHCP 服务，以实现公司所有终端自动配置 IP 地址的需求。确定题目的基本配置意图和配置代码，根据题意，将配置代码补充完整，或选择合适的选项。

**【问题 1】**

该问题考查在路由器上 DHCP 服务器的配置方法和配置代码。

配置步骤如下：

（1）配置 DHCP 地址池；

（2）确定可用于分配给终端的 IP 地址范围，去除掉不分配给客户端的 IP 地址；

（3）设置默认网关地址；

（4）设置 DNS 服务器地址；

（5）设置地址租期。

**【问题 2】**

该问题考查考生对于 DHCP 中继服务的配置方法的掌握程度。

在为不同网段的主机使用 DHCP 服务器分配 IP 地址时，由于 DHCP 发现的报文是以广播的形式发送的，不能够跨网段传播，因此需要使用路由器实现 DHCP 报文的中继，以确保 DHCP 服务器能够接收到网络中其他网段用户发送的 DHCP 发现消息。

**参考答案**

**【问题 1】**

（1）192.168.1.2

（2）255.255.255.0

（3）pool

（4）192.168.2.253

（5）12

（6）192.168.20.0

（7）255.255.255.0

（8）192.168.10.1

（9）192.168.10.10

（10）192.168.10.254

**【问题 2】**

（11）192.168.1.2

（12）trunk

（13）allowed

（14）vlan 10

（15）vlan 20